|  |  |
| --- | --- |
| **Network Security**  Diploma in CSF  Year 3 (2020/21) Semester 5 | Week 4 |
| Practical |
| **Application Identification** | |

## 

**Objectives:**

1. To learn about APP ID’s capability on Palo Alto Firewall.
2. To learn about detecting, monitoring and blocking specific applications on Palo Alto Firewall

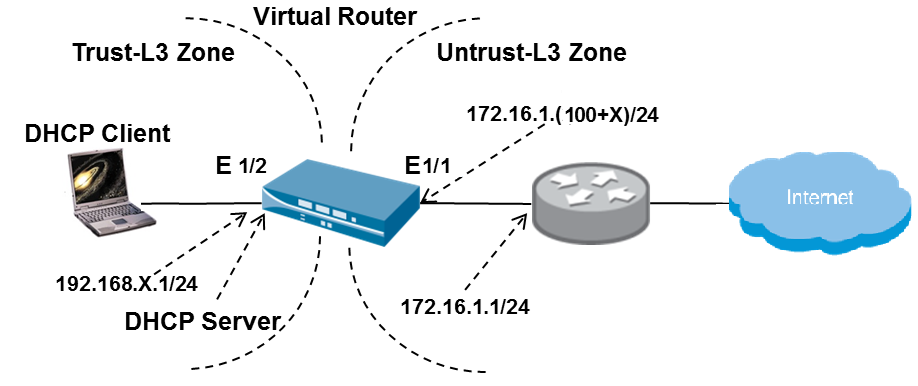
**Instructions:**

1. Configure PC1 with following settings and connect the network port to FW’s MGT port

IP address 192.168.1.2  
Subnet mask 255.255.255.0  
Default gateway: 192.168.1.1

1. Launch browser and type <https://192.168.1.1> at the URL to access FW
2. Login to FW Username: admin, password: admin

5) Setup the firewall with **Layer 3** configuration as follows:



6) Ensure that NAT , DHCP and Virtual Router are configured on the FW.

7) Primary DNS Server: 153.20.62.122

**Part 1: Case Study**

Company ABC has CEO office, HR department, Sales department and IT department. Each department is protected by their own Palo Alto Firewall. As a Network Security Engineer, you are required to create customized Firewall policies for each firewall.

1. Your first step is to develop a Baseline policy that can be applied to all firewalls.

[Baseline policy is the minimum configuration requirement for the firewall]

Follow the below steps to create the policies:

**Create the “General Internet” Policy**

1. Go to the GUI and click **Policies > Security.**
2. Click **Add** to define a security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter General Internet |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust-L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Click **Add** and select each of the following:   * **dns** * **ping** * **ssl** * **web-browsing** |
| **Service/URL Category** tab |  |
| Service | Select **application-default** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Allow** |
| Log Setting | Select **Log at Session Start** |

Click **OK** to close the security policy configuration window.

**Create Policies Block and Log All Inbound and Outbound Traffic**

1. Click **Policies > Security.**
2. Click **Add** to define the Deny Outbound security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Deny Outbound |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust-L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Check the **Any** box |
| **Service/URL Category** tab |  |
| Service | Select **any** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Deny** |
| Log Setting | Select **Log at Session Start** |

Click **OK** to close the security policy configuration window.

1. Click **Add** to define the Deny Inbound security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Deny Inbound |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Untrust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Trust -L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Check the **Any** box |
| **Service/URL Category** tab |  |
| Service | Select **any** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Deny** |
| Log Setting | Select **Log at Session Start** |

Click **OK** to close the security policy configuration window.

1. Ensure your Security Policy looks like this:



1. Click the **Commit** link at the top-right of the GUI. Click **OK** again and wait until the commit process completes before continuing.

**Question A1**: In the “General Internet” rule, why do you use “application-default” as the service, whereas you use “Any” as the service in the two “deny” rules?

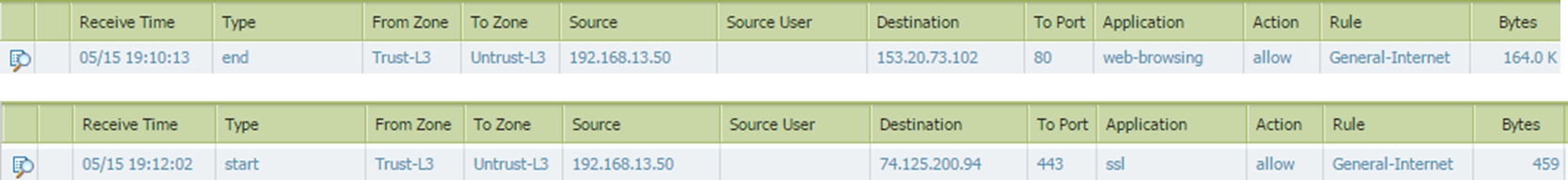
1. Test internet connectivity by browsing websites from your desktop. Does web surfing over ports 80 and 443 work?
2. Attempt to access [www.np.edu.sg](http://www.np.edu.sg) , are you able to access the webpage?

|  |
| --- |
|  |

1. Attempt to access [www.google.com](http://www.google.com) , are you able to access the webpage? Are you able to do a Google search?

|  |
| --- |
|  |

1. From the Firewall configuration UI, go to *Monitor* tab then click *Traffic* under Logs section. You should be able to find some similar traffic logs as shown below.



Explain the important fields of the log.

|  |  |
| --- | --- |
| Source |  |
| Destination |  |
| To Port | 80: |
| 443: |
| Application | Web-browsing: |
| ssl: |
| Action |  |
| Rule |  |

1. Use a browser to connect to the site *http://www.box.net*. The browser should not be able to display the site. Review the traffic logs to determine why this site is not reachable. (Hint: Check the applications listed in the log.) The boxnet-base application is not allowed by the configured policies.
2. Attempt to go to <https://gmail.google.com> , are you able to access it? Why?

|  |
| --- |
|  |

1. The staffs in Sales department are allowed to use Gmail and Google Map due to the nature of the work. Assume the firewall you are configuring now is the one in Sales department. Add one rule for them to access Gmail and Google Map.

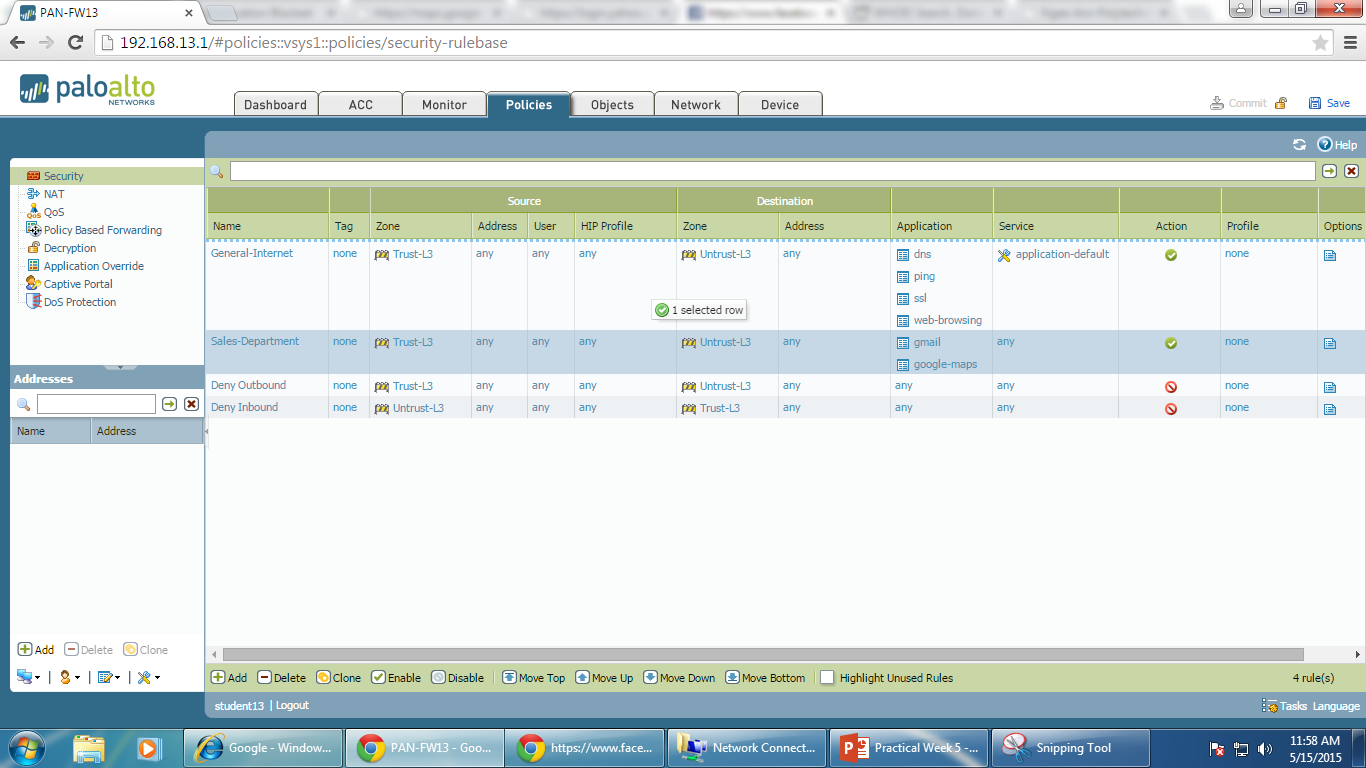
**Create the “Sales-Department” Policy**

1. Go to the GUI and click **Policies > Security.**
2. Click **Add** to define a security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Sales-Department |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust-L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Click **Add** and select the following:   * **Gmail** * **Google-maps** |
| **Service/URL Category** tab |  |
| Service | Select **Any** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Allow** |
| Log Setting | Select **Log at Session Start** |

Click **OK** to close the security policy configuration window.

1. When you reach the below screen, use your mouse to select the row of “Sales-Department” policy and drag it to the top. Ensure “Sales-Department” policy now is above the “Deny Outbound” policy and “Deny Inbound” policy.



1. Commit the changes and then verify that you are now able to access both Gmail and Google Map.
2. The staffs in CEO Office are allowed to use Facebook in addition to Gmail and Google Map. Assume the firewall you are configuring now is the one in CEO Office. Add one rule for them to access Facebook.

**Create the “Allow-Facebook” Policy**

1. Go to the GUI and click **Policies > Security.**
2. Click **Add** to define a security policy:

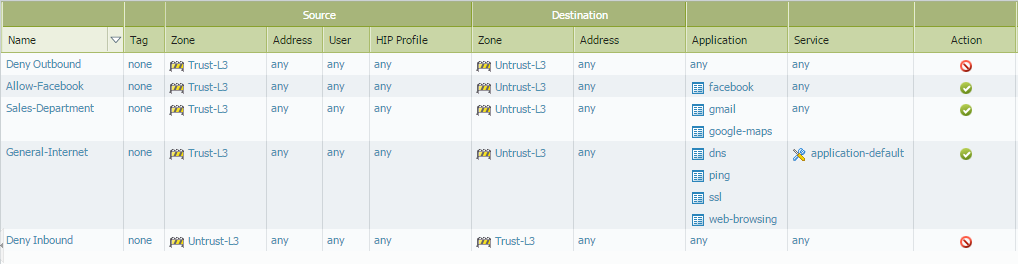
|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Allow-Facebook |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust-L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Click **Add** and select the following:   * **facebook** |
| **Service/URL Category** tab |  |
| Service | Select **Any** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Allow** |
| Log Setting | Select **Log at Session Start** |

Click **OK** to close the security policy configuration window.

1. Ensure your policies screen looks similar to the below, commit the changes and verify that you are able to access Facebook now.



1. Without modifying any policy, just move the “Deny Outbound” policy to the top and commit the changes. Are you still able to access Facebook, Gmail or Google Map? Why?



|  |
| --- |
|  |

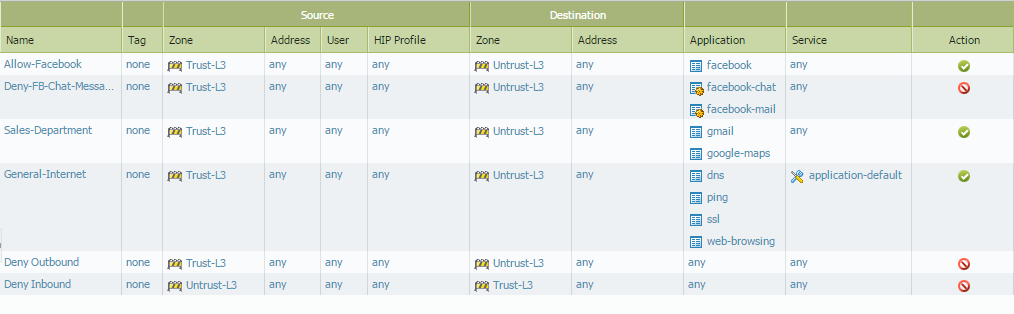
1. The staffs in HR department are allowed to view Facebook page, but not allowed to use Chat and Messaging in Facebook. Create a new policy according to this requirement.

**Create the “Deny-FB-Chat-Messaging” Policy**

1. Create a new policy
2. Click **Add** to define the “Deny-FB-Chat-Messaging” security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Deny-FB-Chat-Messaging |
| **Source** tab |  |
| Source Zone | Click **Add** and select **Trust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust -L3** |
| Destination Address | Any |
| **Application** tab |  |
| Applications | * Facebook-chat * Facebook-mail |
| **Service/URL Category** tab |  |
| Service | Any |
| **Actions** tab |  |
| Action Setting | Deny |
| Log Setting | Select **Log at Session End** |

1. Ensure your policies look like below and commit your changes.



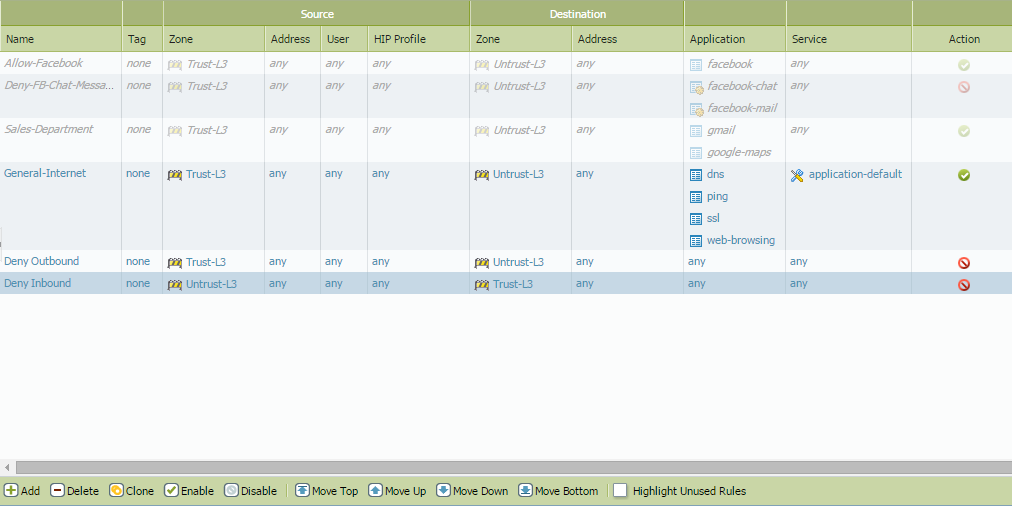
**Question D1**: Were you successful? Why, or why not?

**Question D2**: Why do you think if SSL is enabled, policy does not work?

1. The IT department has confidential data of the company, so there should be no more access right given other than the baseline policy. Configure the firewall back to the initial policy settings.
2. Go to the Policy tab and highlight the three newly created policies:

* Allow-Facebook
* Deny-FB-Chat-Messaging
* Sales-Department

1. Click the “Disable” icon at the bottom the disable the above policies.
2. You policy page should look like below.



1. Verify that you are not able to access Gmail, Facebook, or Google Map.
2. In addition to the above, attempt to access [www.skype.com](http://www.skype.com) , are you able to open the Skype homepage or sign in to Skype?

|  |
| --- |
|  |

**Part 2: Create Application Filters**

1. Go to the GUI and click **Objects > Application Filters.**
2. Click **Add** to define the Proxies application filter:

|  |  |
| --- | --- |
| Name | Enter Proxies |
| **Subcategory** column | Select **proxy** |

Click **OK** to close the application filter configuration window.

1. Click **Add** to define the Web-Based-File-Sharing application filter:

|  |  |
| --- | --- |
| Name | Enter Web-Based-File-Sharing |
| **Subcategory** column | Select **file-sharing** |
| **Technology** column | Select **browser-based** |

Click **OK** to close the application filter configuration window.

**Create Application Groups**

1. Click **Objects > Application Groups**.
2. Click **Add** to define the Known-Good application group:

|  |  |
| --- | --- |
| Name | Enter Known-Good |
| Applications | Click **Add** and select each of the following:   * **dns** * **fileserve** * **flash** * **ftp** * **ping** * **ssl** * **web-browsing** |

Click **OK** to close the application group configuration window.

1. Click **Add** to define the Known-Bad application group:

|  |  |
| --- | --- |
| Name | Enter Known-Bad |
| Applications | Click **Add** and select each of the following:   * **Proxies** * **Web-Based-File-Sharing** |

Click **OK** to close the application group configuration window.

**Update Security Policies**

1. Click **Policies > Security**.
2. Click **General Internet** to edit the existing rule. Go to the **Application** tab. Delete all of the listed applications and add the **Known-Good** application group. Click **OK** to close the window.
3. Click the **Deny Outbound** rule and modify with the following values:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Change to Log-All |
| **Actions** tab |  |
| Action Setting | Select **Allow** |

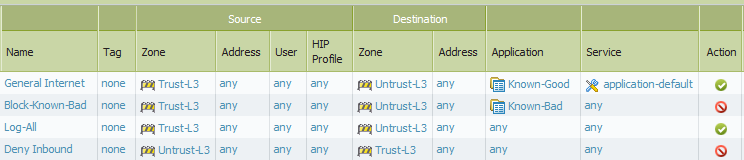
Click **OK** to close the security policy configuration window.

1. Click **Add** to define the Block-Known-Bad security policy:

|  |  |
| --- | --- |
| **General** tab |  |
| Name | Enter Block-Known-Bad |
| **Source** tab |  |
| Source Zone | Click **Add** and select T**rust-L3** |
| Source Address | Select **Any** |
| **Destination** tab |  |
| Destination Zone | Click **Add** and select **Untrust -L3** |
| Destination Address | Select **Any** |
| **Application** tab |  |
| Applications | Click **Add** and select **Known-Bad** |
| **Service/URL Category** tab |  |
| Service | Select **any** from the pull-down |
| **Actions** tab |  |
| Action Setting | Select **Deny** |
| Log Setting | Select **Log at Session End** |

Click **OK** to close the security policy configuration window.

1. Use the move buttons at the bottom of the page to arrange the policies in a logical order. Confirm that your security rule list looks like this:



You can also rearrange the rule by clicking and dragging them into the correct order.

1. Click the **Commit** link at the top-right of the GUI. Click **OK** again and wait until the commit process completes before continuing.

**Verify Internet Connectivity and Application Blocking**

1. Verify that your policies have not broken network connectivity. Test internet connectivity by browsing websites from your desktop. Does web surfing over ports 80 and 443 work?
2. Use a browser to connect to the site *http://www.box.net*. The browser should not be able to display the site. Review the traffic logs to determine why this site is not reachable. (Hint: Check the application listed in the log.)
3. Attempt to reach the site *http://www.box.net* using the proxy site *http://www.avoidr.com*. Why can’t you bring up that web site? (Hint: the traffic logs will help you solve this problem.)
4. Click the **ACC** tab to access the Application Command Center. Use the drop-down menu in the application section of the ACC to select different ways of viewing the traffic that you have generated. What is the total risk level for all traffic that has passed through the firewall thus far? Notice that the URL Filtering, Threat Prevention, and Data Filtering sections within the ACC contain no matching records.

<https://www.paloaltonetworks.com/products/features/decryption.html>

<https://live.paloaltonetworks.com/docs/DOC-1412>