**ASSIGNMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| **COURSE** | PAN Firewall | **ASSIGNMENT NO** | 4 |
| **MODULE** | Firewall | **ASSIGNMENT DATE** | 28-Sep-24 |
| **STUDENT NAME** | Konganti Chaithanya Kumar | **SUBMIT DATE** | 29-Sep-24 |

**1. Steps to Configure Security Profiles: File Blocking and DoS Protection on Palo Alto Firewall**

**A. File Blocking Security Profile Configuration**

**Step 1: Login to the PAN Firewall**

* Open a web browser and navigate to the firewall's IP address.
* Log in with your admin credentials.

**Step 2: Navigate to File Blocking Profile**

* On the web interface, go to **Objects > Security Profiles > File Blocking**.

**Step 3: Create a New File Blocking Profile**

* Click **Add** to create a new File Blocking profile.
* Name the profile (e.g., "File-Block-Policy").

**Step 4: Add Blocking Rules**

* Under **File Blocking Rules**, click **Add**.
* Select the **Application** (e.g., web-browsing, ftp, etc.).
* Select the **File Type** (e.g., PE files, PDF, MS Office, etc.) you want to block.
* Choose the **Action** (e.g., Block or Alert).
* Click **OK** to save.

**Step 5: Attach File Blocking Profile to Security Policy**

* Go to **Policies > Security**.
* Choose an existing Security Policy or create a new one.
* Under the **Actions** tab, apply the newly created File Blocking profile by selecting it from the dropdown.

**Screenshot Example:** *Include a screenshot of the File Blocking profile creation and application in the security policy.*

**B. DoS Protection Security Profile Configuration**

**Step 1: Navigate to DoS Protection Profiles**

* Go to **Objects > Security Profiles > DoS Protection**.

**Step 2: Create a New DoS Protection Profile**

* Click **Add** to create a new DoS protection profile.
* Name the profile (e.g., "DoS-Protection-Policy").

**Step 3: Configure Flood Protection**

* Under the **Flood Protection** section, enable protection against **SYN Flood**, **ICMP Flood**, or **UDP Flood**.
* Set the **Threshold** values based on the traffic load. For example, configure a SYN Flood with a rate of 1000 packets per second.
* Enable **Aggregate** or **Classified** protection based on your requirement.

**Step 4: Apply DoS Protection to a Security Policy**

* Go to **Policies > DoS Protection**.
* Create a new DoS policy and apply the created DoS profile to protect specific zones or IP ranges.

**Screenshot Example:** *Include a screenshot of the DoS protection profile settings and its application in the security policy.*

**2. Packet Capture of Dropped Rule**

**Step-by-Step Packet Capture of Dropped Traffic**

**Step 1: Navigate to Packet Capture Settings**

* Go to **Monitor > Packet Capture** on the web interface.

**Step 2: Create a Packet Capture Filter**

* Click **Add** to create a new packet capture filter.
* Under **Match**, specify the conditions for the packet you want to capture (e.g., source IP, destination IP, application, or port).
* For a dropped packet rule, you can match the IP address or port of the traffic being dropped.

**Step 3: Define Stages to Capture**

* Choose the capture stages: **Firewall stage**, **Receive**, **Transmit**, and **Drop**. For dropped traffic, select **Drop**.

**Step 4: Enable Packet Capture**

* Enable the packet capture by selecting the **Enable** checkbox.
* Click **OK** to save the configuration.

**Step 5: Generate Traffic**

* Generate the traffic that will be dropped by the firewall according to the applied security rule (e.g., by accessing a blocked URL or application).

**Step 6: View and Download Packet Capture**

* Once the traffic is generated and captured, go to **Monitor > Packet Capture**.
* Download the .pcap file for further analysis in tools like Wireshark.

**Step 7: Analyze the .pcap File**

* Open the downloaded .pcap file in Wireshark.
* Look for packets that match the dropped rule criteria, such as TCP resets or dropped connections.

**Screenshot Example:** *Include screenshots of the packet capture filter settings and the .pcap file analysis in Wireshark.*