# Tool Reference: Palo Alto Firewall

## Logging In to both the DMZ and Central Firewalls

Open the Microsoft Edge browser on the desktop of your SOC workstation and click the bookmark for either the DMZ or Central Palo Alto firewall and use the **saved credentials** to

## Monitoring Network Traffic

Once Logged in, clicking the "Monitor" tab at the top of the window will take you directly to the traffic page where you can use the search bar at the top to query through the firewall logs:

**Example Queries:**

(addr.dst in 192.168.1.1) - Shows all traffic going to the specified IP

(addr.src in 192.168.1.2) - Shows all traffic originating from the specified IP

(addr.dst in 192.168.1.1) AND (addr.src in 192.168.1.2) - Shows only traffic starting from source IP specified and going to the destination IP specified.

## Implementing a Rule to block traffic from a specified IP address

**Step 1:** Click on the "Policies" tab at the top of the window to be taken to the list of security rules implemented on the firewall and click the "Add" button located at the bottom of the page.

**Step 2:** Give the rule you're creating a name and an optional description

**Step 3:** Click on the "Source" tab and add the malicious IP, either using any zone or the zone the traffic is originating from

**Step 4:** Click on the "Destination" tab and choose any zone and any address

**Step 5**: Click on the "Actions" tab and choose either **Drop** or **Deny**, **the former to silently drop the request** and the **later to send a message to the source when the traffic is denied**

**Step 6**: You must create a second rule like the first with the attacker's IP in the destination field and the source being any/any to make sure that traffic is blocked both ways.

**Step 7:** Navigate to Monitor > Session Browser and confirm that there is not an active session with the malicious IP. If there is, click the “X” under the “Clear” column of the active session you wish to end