Test Scenarios for Next-Generation Firewall with Wazuh

**Scenario 1: Failed SSH Login Attempts**

- Objective: Test the Wazuh rule for detecting multiple failed SSH login attempts.

- Setup:

- Attempt multiple SSH logins using an incorrect password:

```bash

ssh user@<server-ip>

```

- Use an incorrect password multiple times.

- Check Wazuh for triggered alerts.

- Expected Outcome: Wazuh should detect multiple failed login attempts and generate an alert.

**Scenario 2: Suspicious Network Activity Detection**

- Objective: Test the rule that identifies unusual network activity.

- Setup:

- Simulate network activity with a tool like `nmap`:

```bash

nmap -sS <target-ip>

```

- Verify if Wazuh captures and logs the event.

- Expected Outcome: Wazuh should generate an alert for suspicious network behavior.

**Scenario 3: Active Response for Blocked IPs**

- Objective: Verify Wazuh’s active response mechanism to block suspicious IPs.

- Setup:

- Trigger an alert (e.g., failed SSH logins).

- Check if the active response blocks the source IP.

- Expected Outcome: The source IP should be blocked for a predefined duration.