Integrate Wazuh with Fortinet Firewall

**Step 1: Configure Fortinet to Send Logs to Wazuh**

1. Log in to your Fortinet firewall using the web interface.
2. Go to **Log & Report** > **Log Settings**.
3. Enable **Syslog** and configure the following:
   * **Server**: Wazuh Manager IP
   * **Port**: 514 (default for syslog)
   * **Format**: CEF (Common Event Format) or JSON
4. Save the changes.

Alternatively, run the following CLI commands on the Fortinet device:

bash

CopyEdit

config log syslogd setting

set status enable

set server <WAZUH\_MANAGER\_IP>

set port 514

set format cef

end

**Step 2: Configure Wajuh to receive logs**

1. Addthe following code on wazuh configuration file in < ossec config> tag.

<!-- syslog -->

<remote>

<connection>syslog</connection>

<port>514</port>

<protocol>udp</protocol>

<allowed-ips>firewall ip</allowed-ips>

</remote>

1. Save the configuration file and restart the wazuh manger.