Setting up Check Point Firewall-1 Collector

https://campus.barracuda.com/doc/99621437/

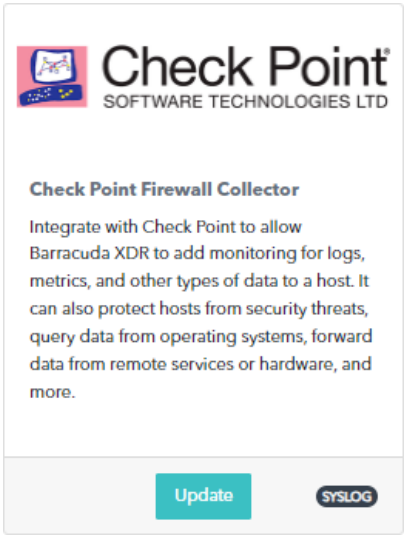
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating Check Point FireWall-1 Monitoring.

To set up Check Point Firewall-1 Collector, do the following steps, below:

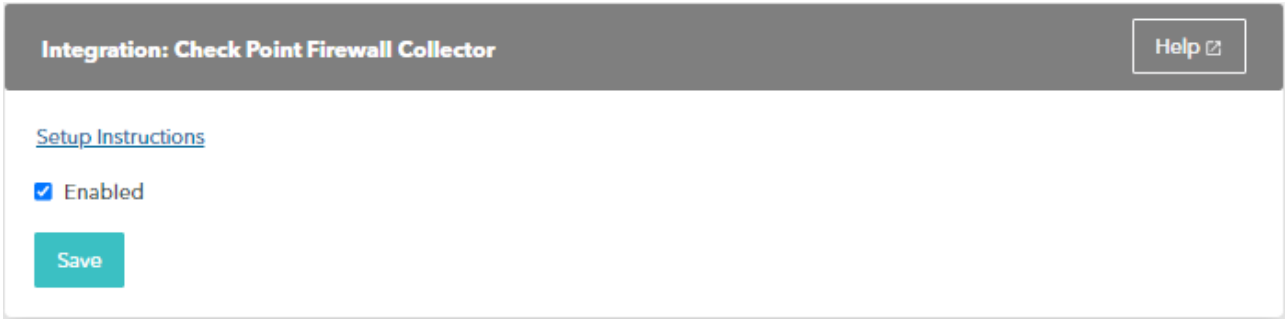
- **Enable Check Point Firewall Collector**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open the port on the XDR Collector Host**

Enable Check Point Firewall Collector

1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **Check Point Firewall Collector** card, click **Setup**.



3. Select the **Enable** check box.



4. Click **Save**.

Install the XDR Collector

When collecting logs from one or more integrated data sources, always set up the XDR Collector on a dedicated host server. Don't use an existing server because the amount of data produced by logs can impact critical infrastructure.

- If you haven't already set up the XDR Collector, do one of the following:
  - Setting up the XDR Collector for Windows
  - Setting up the XDR Collector for Linux

Configuring the Firewall

In Check Point, the **Logs & Monitoring** > **Log Servers** page lets you configure external log servers for security and system logs for additional logging storage.

External Syslog Server Configuration

You can configure a gateway to send logs to multiple external syslog servers.

To configure an external syslog server

1. In **Check Point**, under **Syslog Servers**, click **Configure**.
   The External Syslog Server window opens.
2. Enter a **Name** and **IP address**.
3. Enter a **Port** (9201).
4. Select **Enable log server**.
5. Optionally, select **Show Obfuscated Fields**.
   Obfuscated packets are shown as plain text.
6. Select logs to forward:
   - **System logs**
   - **Security logs**
   - **Both system and security logs**
7. Click **Apply**.
   Documentation Link

Open the Port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9201.

Linux

```
sudo ufw allow 9201/udp
```

Windows

```
netsh advfirewall firewall add rule name="Check Point Firewall Events" dir=in
action=allow protocol=UDP localport=9201
```

Figures