Setting up Palo Alto Collector

https://campus.barracuda.com/doc/99621475/

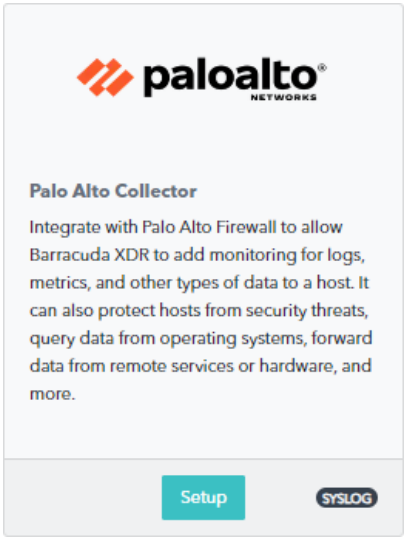
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to Integrating Palo Alto Firewall Logs.

To set up Palo Alto Collector, follow the procedures below:

- **Enable Palo Alto Collector**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open port on the XDR Collector Host**

Enable Palo Alto Collector

1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **Palo Alto** 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

Configure the Firewall

1. In the **Palo Alto Dashboard**, you can define Syslog servers by clicking **Device** > **Server Profiles** > **Syslog**.
2. Click **Add,** then enter a **Name** for the profile.
3. If the firewall has more than one virtual system (vsys), select the **Location** (*vsys* or *Shared*) where this profile is available.
4. For each syslog server, click **Add** and enter the information that the firewall requires to connect to it:
   - **Name**—Unique name for the server profile.
   - **Syslog Server**—IP address or fully qualified domain name (FQDN) of the syslog server. If you configure an FQDN and use UDP transport, if the firewall cannot resolve the FQDN, the firewall uses the existing IP address resolution for the FQDN as the Syslog Server address.
   - **Transport**—Select TCP, UDP, or SSL (TLS) as the protocol for communicating with the syslog server. For SSL, the firewall supports only TLSv1.2.
   - **Port**—The port number on which to send syslog messages (default is UDP on port 9203); you must use the same port number on the firewall and the syslog server.
   - **Format**—Select the syslog message format to use: BSD (the default) or IETF. Traditionally, BSD format is over UDP and IETF format is over TCP or SSL/TLS.
   - **Facility**—Select a syslog standard value (default is LOG_USER) to calculate the priority (PRI) field in your syslog server implementation. Select the value that maps to how you use the PRI field to manage your syslog messages.
5. (Optional) To customize the format of the syslog messages that the firewall sends, click the **Custom Log Format** tab.

   For details on how to create custom formats for the various log types, refer to the Common Event Format Configuration Guide.
6. Click **OK**.

For more information, see the Palo Alto Documentation.

Open the Port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9203.

Linux

```
sudo ufw allow 9203/udp
```

Windows

```
netsh advfirewall firewall add rule name="Palo Alto Firewall Events" dir=in
action=allow protocol=UDP localport=9203
```

Figures

1. 2024-02-29_13-16-27.png
2. 2024-02-29_13-17-02.png