Setting up Cisco FTD Collector
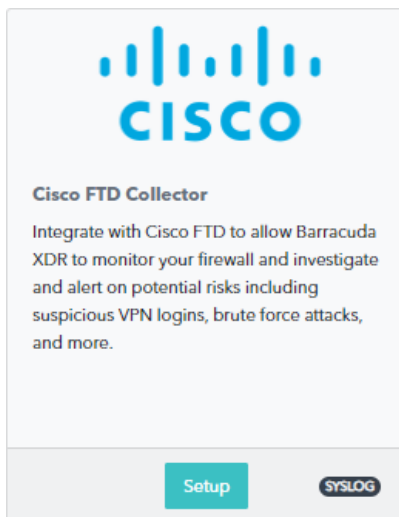
https://campus.barracuda.com/doc/101712546/

To set up Cisco FTD collector, do the following:

- **Enable Cisco FTD collector**
- **Install the XDR Collector**
- **Configure Cisco FTD**
- **Open the port on the XDR Collector Host**

Enable Cisco FTD collector

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

3. Select the **Enabled** 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

To consult the Cisco documentation, see Configure Logging on FTD via FMC.

1. Log in to your **Firepower Managed Center** console.
2. Click **Devices**.
3. Click **Platform settings**.
4. Navigate to **Threat Defense Policy** > **Syslog** > **Syslog Servers**.
5. For **Protocol**, select **UDP**.
6. For **Port**, type **9222**.
7. To save the configuration, click **OK** and **Save**.
8. To save the platform, click **Save**.
9. Select **Deploy**.
10. Choose the FTD appliance where you want to apply the changes.
11. Click **Deploy**.

Open the Port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9222.

Linux

```
sudo ufw allow 9222/udp
```

Windows

```
netsh advfirewall firewall add rule name="Cisco FTD Firewall Events" dir=in
action=allow protocol=UDP localport=9222
```

Figures

1. 2024-02-29_11-21-37.png
2. 2024-02-29_11-22-29.png