Setting up Fortinet FortiGate Firewall Collector

https://campus.barracuda.com/doc/99621455/

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

To set up Fortinet FortiGate Firewall Collector, do the following procedures, below:

- **Enable Fortinet FortiGate Firewall Collector**
- **Install the XDR Collector**
- **Configure the firewall**
- **Open the port on the XDR Collector Host**

Enable Fortinet FortiGate Firewall Collector

1. In **Barracuda XDR Dashboard**, navigate to **Administration** > **Integrations**.
2. On the **Fortinet FortiGate Firewall Collector** card, click **Setup**.
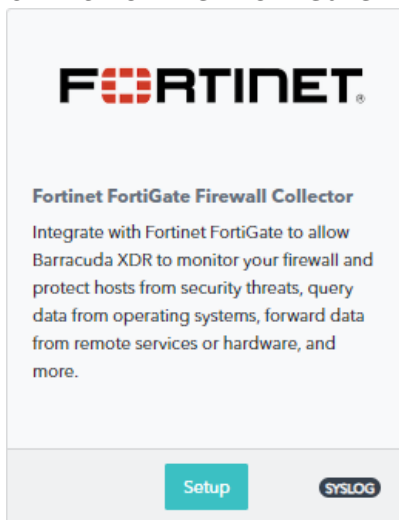
3. Select the **Enable** check box.

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

- Log into the FortiGate command line and run the command below, where <X.X.X.X> is the IP address of the Collector:
  ```
  config log syslogd setting
  set status enable
  set server <X.X.X.X>
  set mode udp
  set port 9202
  set facility local7
  end
  ```

The Fortinet FortiGate Firewall syslog settings documentation can be found here.

Open the Port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9202.

Linux

```
sudo ufw allow 9202/udp
```

Windows

```
netsh advfirewall firewall add rule name="Fortinet FortiGate Firewall Events"
dir=in action=allow protocol=UDP localport=9202
```

Figures

1. 2024-02-29_13-13-13.png
2. 2024-02-29_13-13-28.png