

Fortinet-Fortigate Integrations

Introduction

This integration is for Fortinet FortiGate logs sent in the syslog format.

Pre-requisite:

Configure syslog on FortiGate

From the GUI:

1. Log into **FortiGate**.
2. Select **Log & Report** to expand the menu.

3. Select **Log Settings**.

The screenshot displays the Fortinet management console interface. On the left, the 'Log & Report' menu is expanded, and 'Log Settings' is selected. The main content area shows the 'Log Settings' configuration page. A red box highlights the 'Send logs to syslog' toggle switch, which is currently turned off. Below this, the 'Cloud Logging Settings' section is visible, showing 'FortiGate Cloud' as the selected type, 'Connected' as the connection status, and 'Real Time' as the upload option. A bar chart titled 'Logs Sent to FortiGate Cloud Daily' displays the volume of logs sent over a period from August 02 to August 08. The chart shows two data series: Traffic Log (orange) and Event Log (grey). The y-axis represents the volume in MB, ranging from 0.00 MB to 12.00 MB. The x-axis shows the dates from Aug 02 to Aug 08. The chart indicates that the total logs sent are approximately 10 MB per day, with Traffic Log accounting for about 4 MB and Event Log for about 6 MB.

Date	Traffic Log (MB)	Event Log (MB)	Total (MB)
Aug 02	4.0	6.0	10.0
Aug 03	4.0	6.0	10.0
Aug 04	3.0	6.0	9.0
Aug 05	3.0	6.0	9.0
Aug 06	3.0	6.0	9.0
Aug 07	4.0	6.0	10.0
Aug 08	6.0	3.0	9.0

4. Toggle Send Logs to Syslog to **Enabled**.

5. Enter the Syslog Collector **IP address**. Note: IP Address must be **host's IP Address** where the **Elastic-Agent is installed**. (For example. 192.168.1.19 as shown below)

The screenshot displays the FortiGate web interface for Log Settings. The left sidebar contains a navigation menu with categories like Network, Policy & Objects, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, System, Security Fabric, and Log & Report. The 'Log & Report' section is expanded, showing options like Forward Traffic, Local Traffic, Sniffer Traffic, Events, AntiVirus, Web Filter, SSL, DNS Query, File Filter, Web Application Firewall, Application Control, Intrusion Prevention, Anomaly, Anti-Spam, FortiGate Cloud Reports, Log Settings (selected), and Threat Weight.

The main content area is titled 'Log Settings'. It features a 'Send logs to syslog' toggle switch which is turned on. Below this, there is a text field for 'IP Address/FQDN' containing the value '192.168.1.19'. Further down, the 'Cloud Logging Settings' section is visible, showing 'Type' as 'FortiGate Cloud', 'Connection status' as 'Connected', 'Upload option' as 'Real Time', and 'Region' as 'GLOBAL'. A bar chart titled 'Logs Sent to FortiGate Cloud Daily' shows the volume of logs sent over the last 7 days. An 'Apply' button is located at the bottom right of the settings area.

If it is necessary to customize the port or protocol or setup the Syslog from the CLI below are the commands:

```
config log syslogd setting
```

```
    set status enable
```

```
    set server "192.168.1.19" -- change IP Address to same as host's where Elastic Agent is installed
```

```
    set mode udp
```

```
    set port 514
```

```
end
```

```
~ (setting) # sh f
config log syslogd setting
  set status enable
  set server "192.168.1.19"
  set mode udp
  set port 514
  set facility local7
  set source-ip ''
  set format default
  set priority default
  set max-log-rate 0
  set interface-select-method auto
end
```

To establish the connection to the Syslog Server using a specific Source IP Address, use the below CLI configuration:

```
config log syslogd setting
  set status enable
  set server "192.168.1.19" -- change ip address to match host's IP
  set source-ip "172.16.1.1" -- change ip address to match host's source-ip
address

  set mode udp

  set port 514
end
```

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Compatibility

This integration has been tested against FortiOS versions 6.x and 7.x up to 7.4.1. Newer versions are expected to work but have not been tested.

Note

- When using the TCP input, be careful with the configured TCP framing. According to the [Fortigate reference](#), framing should be set to `rfc6587` when the syslog mode is reliable.

Fortinet FortiGate Integration Procedures

Please provide the following information to **CyTech**:

Collect Fortinet FortiGate logs (input: tcp)

1. Listen Address - The bind address to listen for TCP connections.
2. Listen Port - The TCP port number to listen on.

Collect Fortinet FortiGate logs (input: udp)

1. Listen Address - The bind address to listen for UDP connections.
2. Listen Port - The UDP port number to listen on.

If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Revision #5

Created 23 April 2024 12:56:55

Updated 21 October 2024 08:07:08 by David Napoleon Romanillos