

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 shows the Fortinet Log Settings page. The left sidebar has 'Log & Report' expanded, with 'Log Settings' highlighted. The main content area shows 'Log Settings' with a 'Send logs to syslog' toggle set to 'Off'. Below this is the 'Cloud Logging Settings' section, which includes options for 'Type' (FortiGate Cloud), 'Connection status' (Connected), 'Upload option' (Real Time), 'Account', and 'Region' (GLOBAL). A bar chart titled 'Logs Sent to FortiGate Cloud Daily' shows data from Aug 02 to Aug 08, with 'Traffic Log' in orange and 'Event Log' in grey. The 'Apply' button is at the bottom right.

Date	Traffic Log (MB)	Event Log (MB)
Aug 02	4.0	5.5
Aug 03	3.8	5.8
Aug 04	3.0	6.0
Aug 05	3.2	6.0
Aug 06	3.2	6.0
Aug 07	4.0	6.0
Aug 08	6.5	3.0

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 management console's 'Log Settings' page. The left sidebar shows the navigation menu with 'Log Settings' selected. The main content area includes a 'Log Settings' section with a 'Send logs to syslog' toggle set to 'On' and an 'IP Address/FQDN' field containing '192.168.1.19'. Below this is the 'Cloud Logging Settings' section, where 'FortiGate Cloud' is selected as the type, and the connection status is 'Connected'. The upload option is set to 'Real Time'. A bar chart titled 'Logs Sent to FortiGate Cloud Daily' shows the volume of logs sent over a period of days. An 'Apply' button is located at the bottom right of the interface.

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