# Fortinet-Fortigate Integrations

## Introduction

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

---

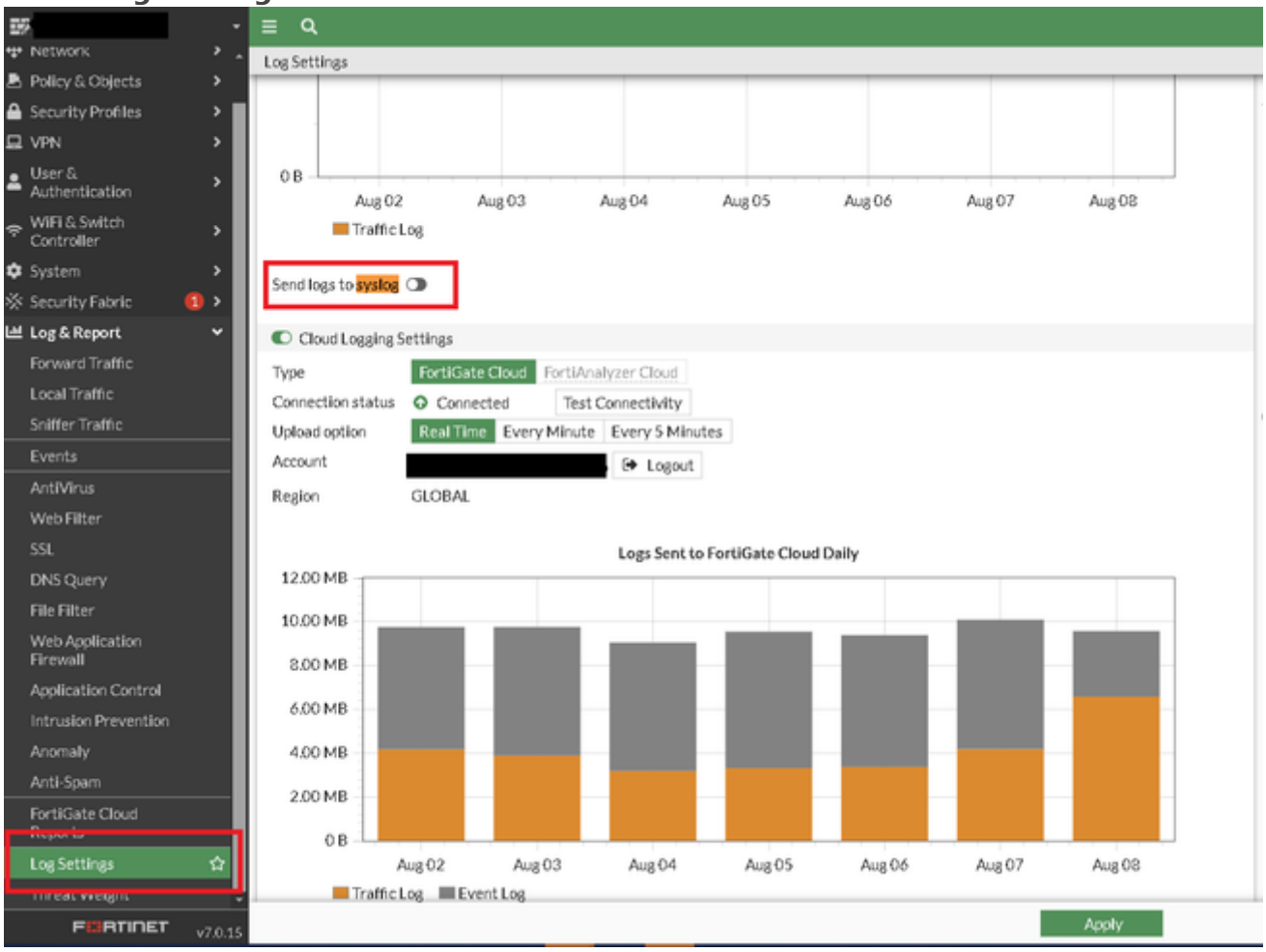
## Pre-requisite:

### Configure syslog on FortiGate

From the GUI:

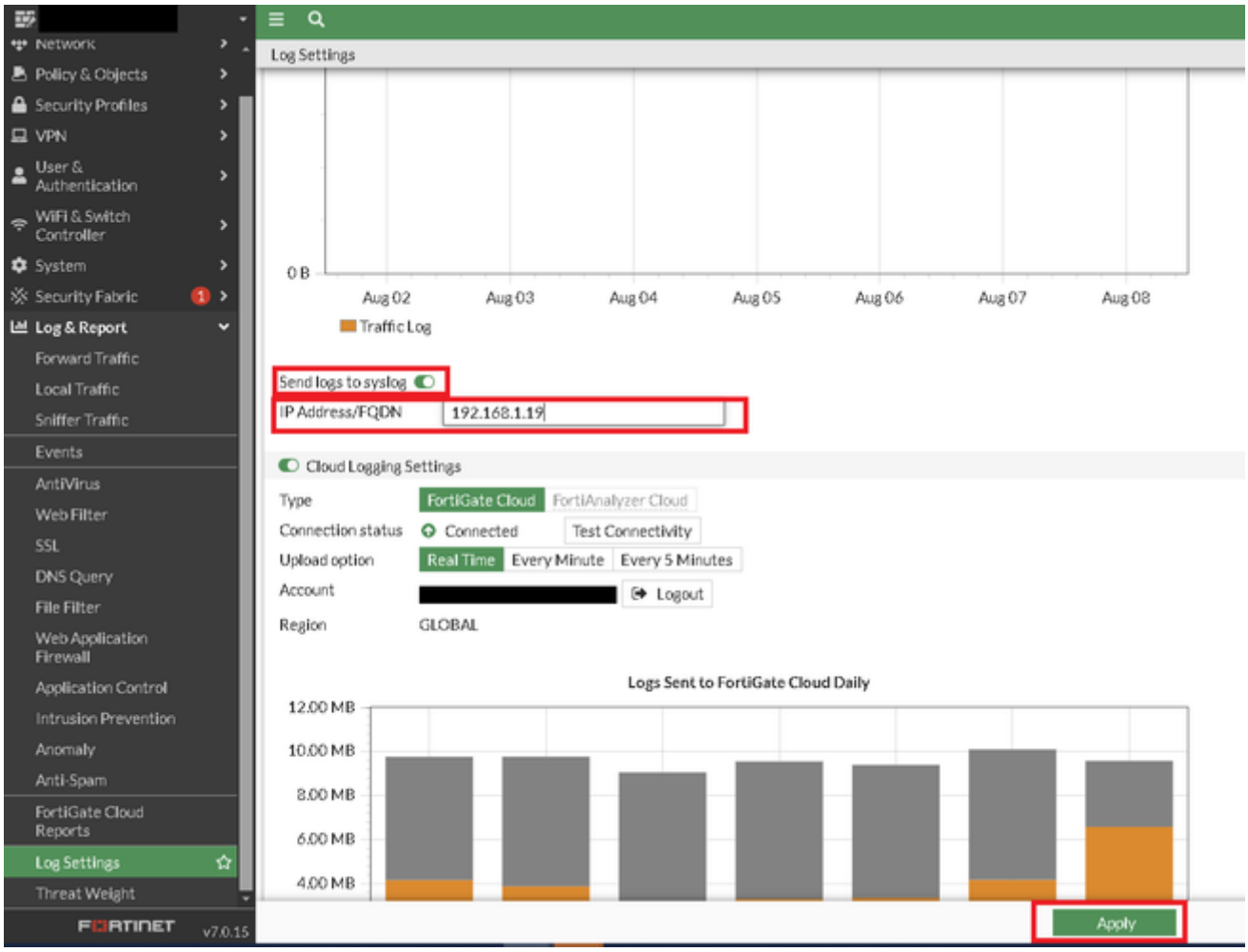
1. Log into **FortiGate.**
2. Select **Log & Report** to expand the menu.

3. Select **Log Settings.**



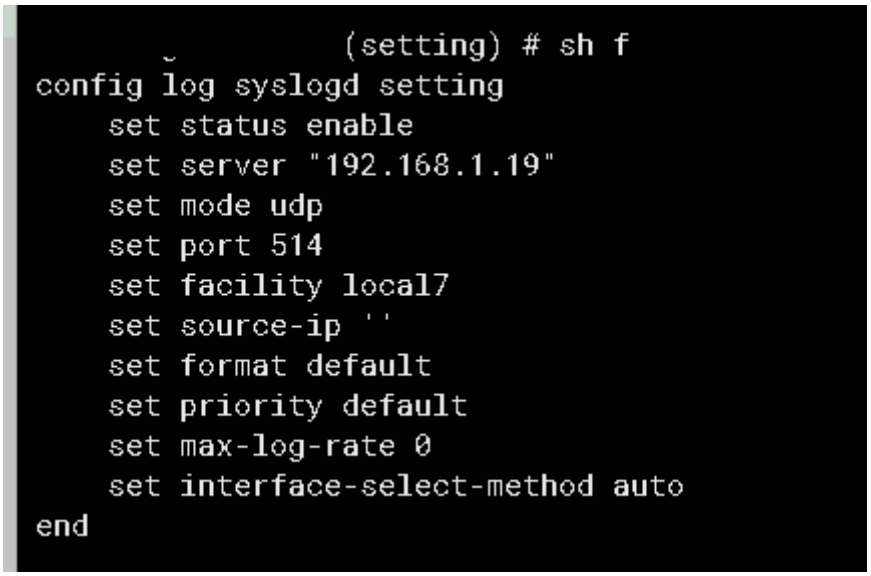

4. Toggle Send Logs to Syslog to **Enabled.**

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)




**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
```




**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