Fortinet-Fortigate Integrations

Introduction

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

Assumptions

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

Compatibility

This integration has been tested against FortiOS version 6.0.x and 6.2.x. Versions above this are expected to work but have not been tested.

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.

Revision #2
Created 23 April 2024 12:56:55
Updated 19 June 2024 06:54:01