EventTracker

Actionable Security Intelligence

How to – Configure Fortinet Firewall to forward logs to EventTracker

EventTracker

Publication Date: September 17, 2018

Abstract

This guide provides instructions to configure Fortinet Firewall to send crucial events to EventTracker by means of syslog.

Audience

Fortinet Firewall users, who wish to forward it's events to EventTracker Manager and monitor them using EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker version 9.X and later**, and **Fortinet Firewall with FortiOS version 4.0-6.0 or later**.

The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. EventTracker MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from EventTracker, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

EventTracker
Actionable Security Intelligence

Overview

Fortinet Firewall is one of the fastest firewall providing protection in various areas with other key security features such as anti-virus, intrusion prevention system (IPS), web filtering, anti-spam and traffic shaping to deliver multi-layered security for the IT environment.

EventTracker collects and analyses firewall events and enlightens an administrator about security violations, user behavior, and traffic anomalies.

Prerequisites

- **EventTracker Agent 9.x** should be installed.
- **Fortinet Firewall** with **FortiOS version 4.0-6.0** should be installed.

Enable Syslog Forwarding in FortiOS version 4.0-5.X

Syslog is a standard for forwarding log messages in an IP network. Syslog captures log information provided by network devices.

1. Connect to your firewall using an SSH/Telnet client.
2. Login using administrative credentials for the firewall.
3. Type in the below commands in the CLI,

```
# config log syslogd setting
Note: If one syslog server is already configured, use syslogd2 or syslogd3 instead. Up to 5 syslog servers can be configured.
        # set status enable
        # set server <EventTracker_Agent_IP>
        (e.g. # set server 192.168.1.52)
        # set port 514
        # set csv enable
# end
# config log syslogd filter
        # set severity information
# end
```


EventTracker
Actionable Security Intelligence

Enable Syslog Forwarding in FortiOS version 6.0

1. Connect to your firewall using an SSH/Telnet client with administrative privileges or directly from the **Fortinet** web interface as shown in the below image.

2. Click on the **CLI option** as highlighted in the below image.

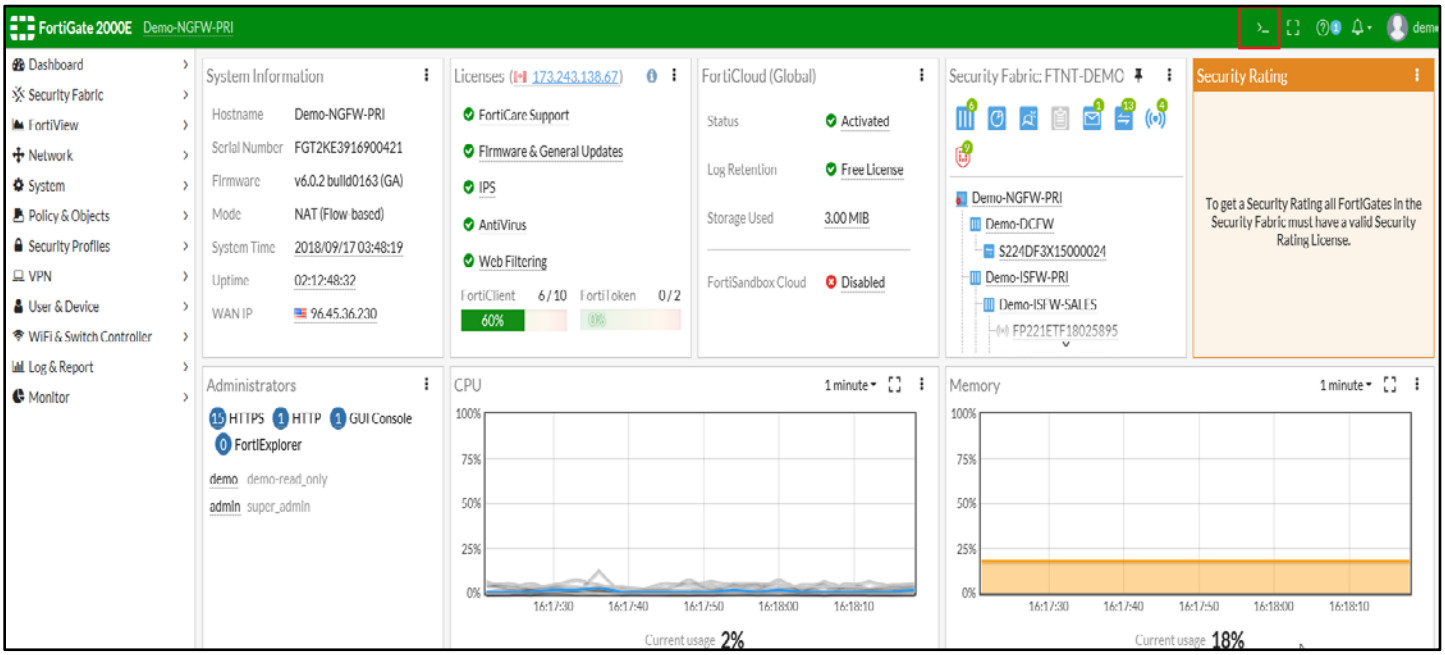

Figure 1

3. CLI window will show up as seen below.

EventTracker
Actionable Security Intelligence

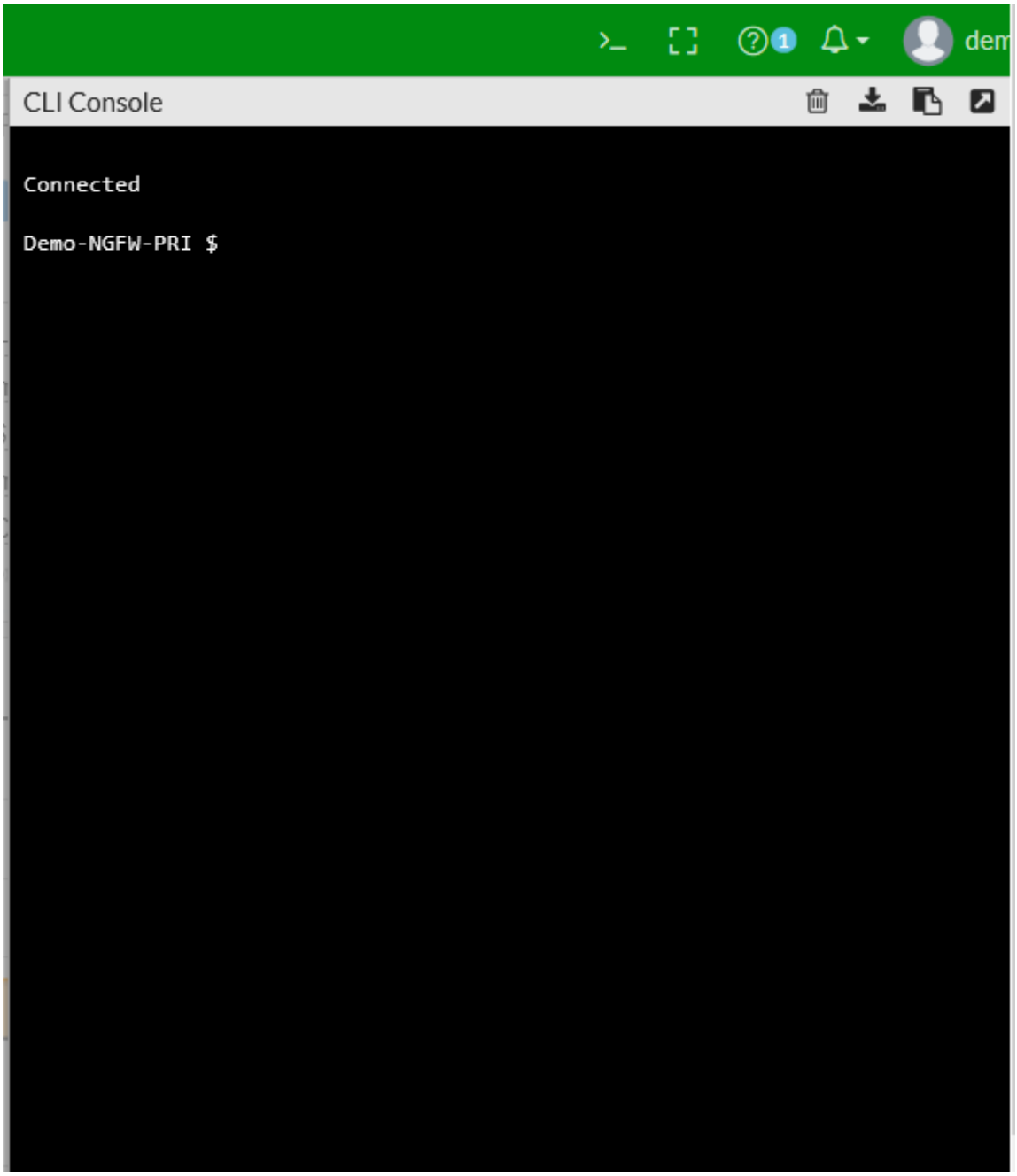

Figure 2

4. Type in the below commands in the CLI,

```
# config log syslogd setting
Note: If one syslog server is already configured, use syslogd2 or syslogd3 instead. Up to 5 syslog servers can be configured.
        # set status enable
```


EventTracker
Actionable Security Intelligence

```
        # set server <EventTracker_Agent_IP>
        (e.g. # set server 192.168.1.52)
        # set mode udp
        # set port 514
        # set format csv
# end
# config log syslogd filter
        # set severity information
# end
```


EventTracker
Actionable Security Intelligence