Netsurion | EventTracker®

How to- Configure Cisco FTD to forward logs to EventTracker

EventTracker v9.x and later

Publication Date: April 15, 2020

Abstract

This guide provides instructions to retrieve the **Cisco FTD** events by syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **Cisco FTD**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **Cisco Firepower release** 6.3 and above**.**

Audience

Administrators who are assigned the task to monitor **Cisco FTD** events using EventTracker.

Table of Contents

1. Overview

Cisco Firepower Threat Defense is an integrative software image combining CISCO ASA and Firepower feature into one hardware and software inclusive system.

The Cisco Firepower NGIPS is a next generation intrusion prevention system. It shares a management console with the Cisco firewall offerings, called the Firepower Management Center.

EventTracker, when integrated with Cisco Firepower NGIPS, collects log from Cisco FTD and creates a detailed reports, alerts, dashboards and saved searches. These features of EventTracker helps users to view the critical and important information on a single platform.

Reports will contain of activities like, IDS events. (which outlines the targeted host and source of attack. Reports also consists of events of activities such as SSLVPN/ VPN/ WebVPN access, user command execution, and system activities.

IPS events include Blocked connections, File and Malware detection summary, Allowed URL's summary, and many more. It includes information such as, date, time, the type of exploit, and contextual information about the source of the attack and its target.

Alerts are provided as soon as any critical event is triggered by Cisco FTD. With alerts users will be able to get real time occurrences of events such as, possible attack that is will be carried out, SSLVPN/ VPN/ WebVPN login success, failures and logout events.
For IPS event, connection blocked due to malicious entity is discovered by NGIPS engine, alerts are directly sent to their email services.

Visual/graphical representation consists of events such as blocked/ allowed connections, security event summary count, and geo-location information which can be viewed on EventTracker 'dashboard'.
Dashboard also displays events related to IDS such as the time of possible attacks from unknown or suspicious sources, information about suspicious URLs, Files, SSL Flow Status, threat name, SHA Disposition, source IP address, and Protocol/service used for establishing connection with FTD etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- EventTracker knowledge packs are required.
- Enable external logging on your Cisco Firepower appliance (for 'connection events' as well as security events such as 'Intrusion' and 'File Malware' Events).

3. Integrating Cisco FTD with EventTracker

Cisco FTD can be integrated with EventTracker using “syslog” forwarding.

3.1 Configuring a Syslog Server

1. Login to your appliance dashboard Choose **Device > Platform Setting > Threat Defense Policy/New Policy**. E.g.

Figure 1

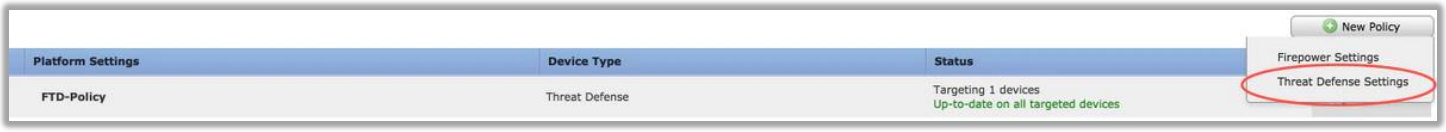

Figure 2

2. Select **Syslog > Syslog Server**.

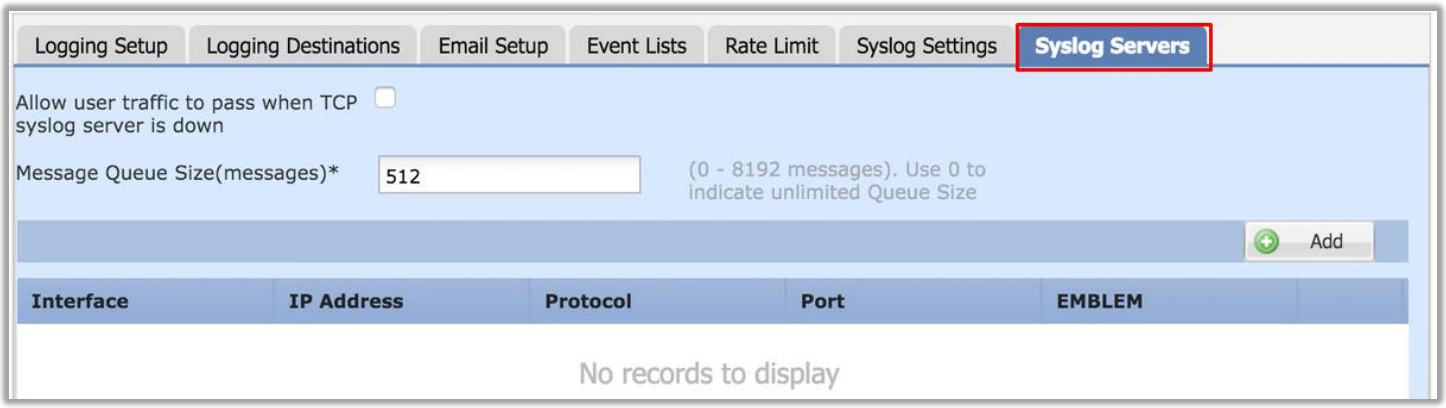

Figure 3

3. Check the **Allow user traffic to pass when TCP syslog server is down** check box, to allow traffic if any syslog server that is using the TCP protocol is down.
4. Enter a size of the queue for storing syslog messages on the security appliance when syslog server is busy in the Message queue size (messages) field. The minimum is 1 message. The default is 512. Specify 0 to allow an unlimited number of messages to be queued (subject to available block memory).

5. Click **Add** to add a new syslog server.

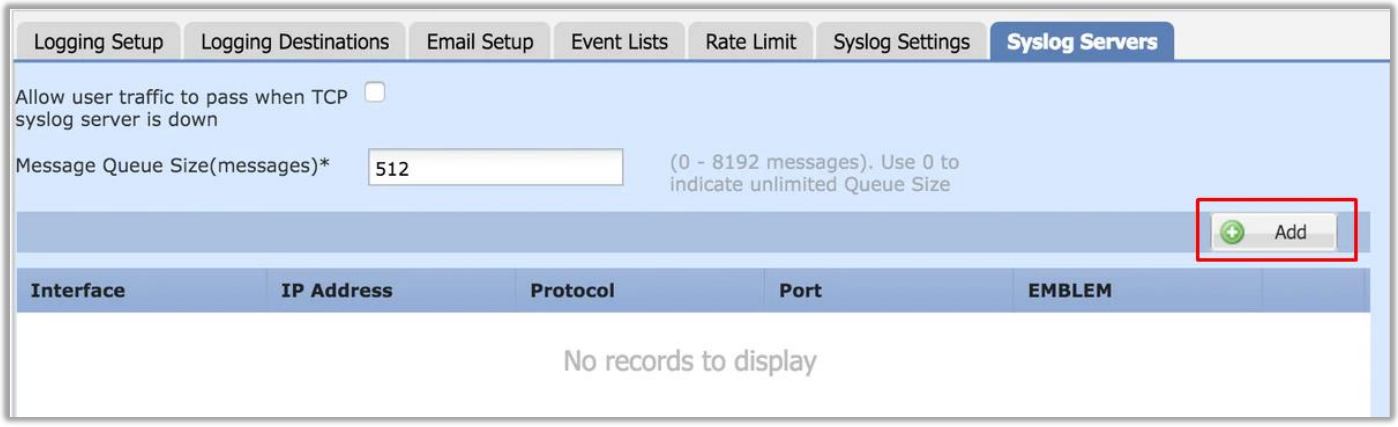

Figure 4

6. Fill-in the details:

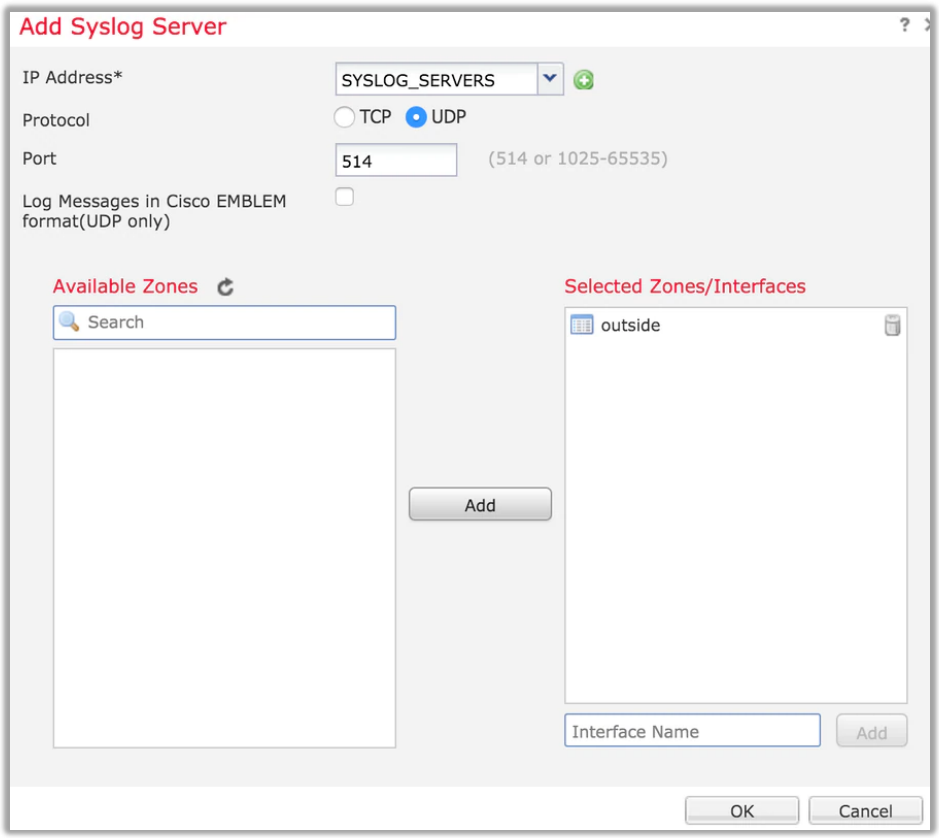

Figure 5

a. In the IP Address drop-down list, select a network host object that contains the IP address of the syslog server.

b. Choose the protocol **UDP** and enter the port number **514** for communications between the Firepower Threat Defense device and the syslog server.
c. Check the **Log messages in Cisco EMBLEM format (UDP only)** check box.
d. Enter the security **zones** over which the Syslog server is reachable and move it to the Selected Zones/ Interfaces Column.
e. Click **OK** and **Save** in order to save the configuration.
f. Click **Save** in order to save the platform setting. Choose **Deploy**, choose the FTD appliance where you want to apply the changes, and click **Deploy** in order to start deployment of the platform setting.