Netsurion™ | EventTracker

How to – Configure WatchGuard XTM to forward logs to EventTracker

EventTracker v9.x or above

Publication Date: July 24, 2019

Abstract

This guide provides instructions to configure WatchGuard XTM to send the event logs to EventTracker. Once events are configured to send to EventTracker alerts, dashboard and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and WatchGuard XTM Fireware v12.5

Audience

WatchGuard XTM users, who wish to forward event logs to EventTracker and monitor events using EventTracker.

Table of Contents

Overview

WatchGuard XTM Series appliances combine firewall/VPN with powerful security services and a suite of flexible management tools.

EventTracker continually collects firewall events and leverages machine learning to identify possible attacks, suspicious network traffic and user behavior analytics.

Prerequisites

- EventTracker v9.x and later should be installed.
- Fireware OS v12.5 or later should be deployed and configured.
- User must have device Administrator access credentials for the WatchGuard XTM and EventTracker.
- Port 514 must be opened on WatchGuard XTM.
- Port 514 must not be used by other services of WatchGuard XTM.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.

Configure syslog forwarding to EventTracker

To collect events from Fireware OS, you must configure your Firebox to send events to EventTracker. You can use Policy Manager or Fireware Web UI to make the changes. In this Integration Guide, we are using Web UI.

Follow the below steps to configure syslog forwarding to EventTracker.

1. Login to Fireware Web UI.
2. Select **System** from left side pane.
3. Select **Logging** and then click the **Syslog Server** tab.

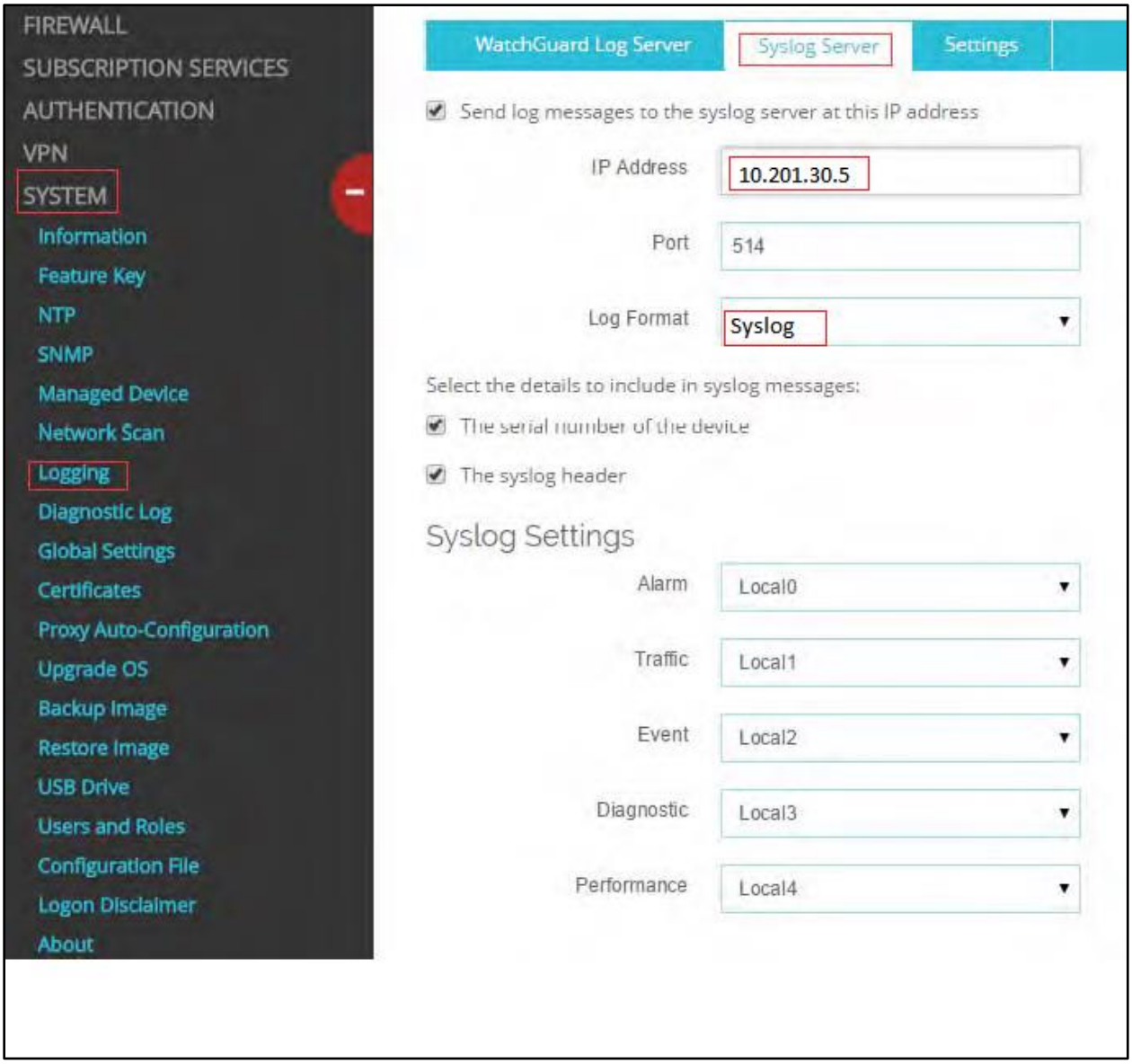

Figure 1

4. In the syslog Server section, select the **Send log messages to the syslog server at this IP address** check box.
5. In the **IP Address** text box, type the IP address of the **EventTracker Agent** machine.
6. In the **Port** text box, type 514.
7. From the **Log Format** drop-down list, select "**syslog**".
8. Select both check boxes '**The serial number of the device'** and '**The syslog header**'.
9. In the syslog Settings section, ensure each log level is assigned a facility.
10. Click **Save**.
11. Go to **Diagnostic Log** under **System.**

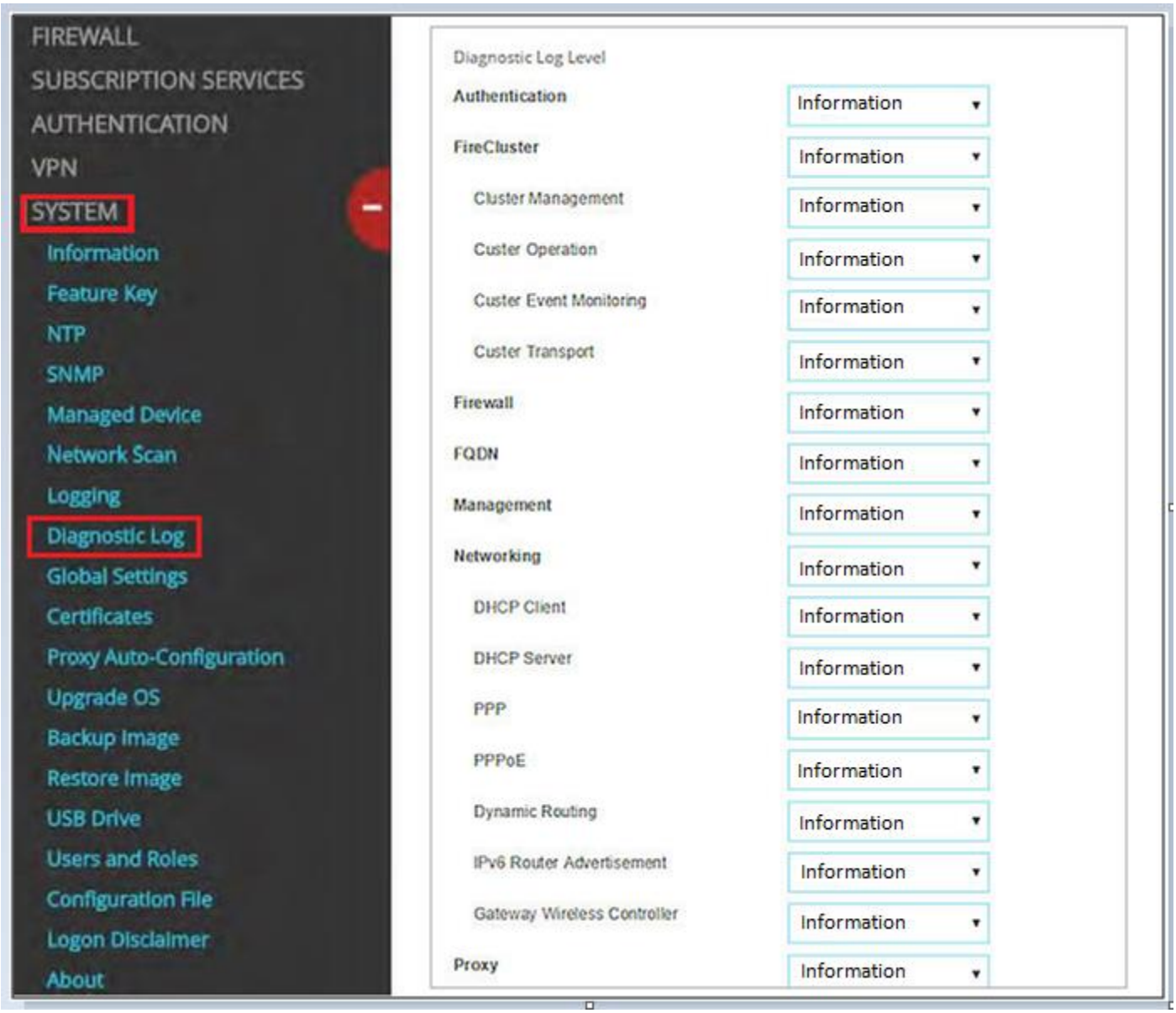

Figure 2

12. In **Diagnostic Log Level**, select **Information** from the drop-down list for each log type.
13. Click **Save**.