Integration Guide

Splunk

Revised: 11 March 2016

About This Guide

Guide Type

Documented Integration — WatchGuard or a Technology Partner has provided documentation demonstrating integration

Guide Details

WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

Splunk Integration Overview

This document describes the steps to integrate Splunk with your WatchGuard Firebox so that the Splunk administrator can index syslog messages sent from the Firebox.

Platform and Software

The hardware and software used to complete the steps outlined in this document include:

- Firebox or WatchGuard XTM device installed with Fireware v11.10.x
- Splunk Enterprise 6.3 installed on a Windows 2012r2 computer

Configuration

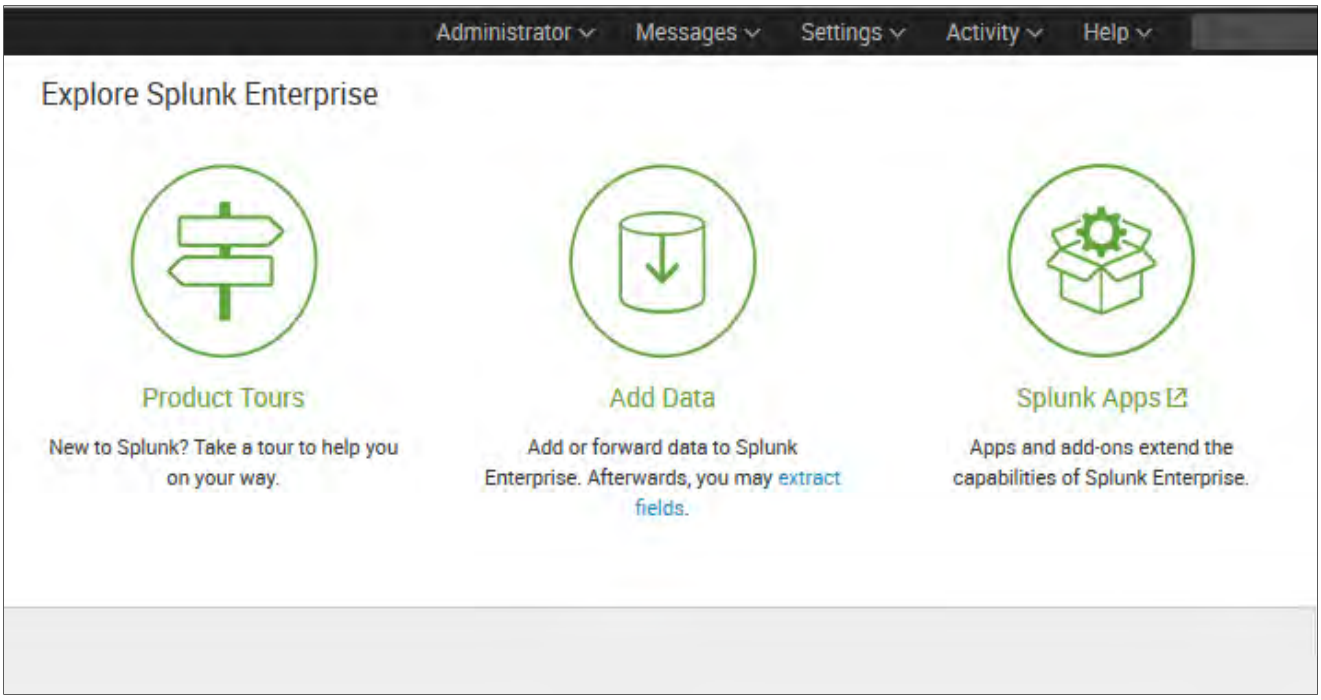
To complete this integration, you must first deploy Splunk Enterprise software.

To set up the Splunk environment, please refer to the Splunk Installation Guide. In this document, we describe the procedure to listen, receive, and index syslog data from the Firebox on Splunk Enterprise.

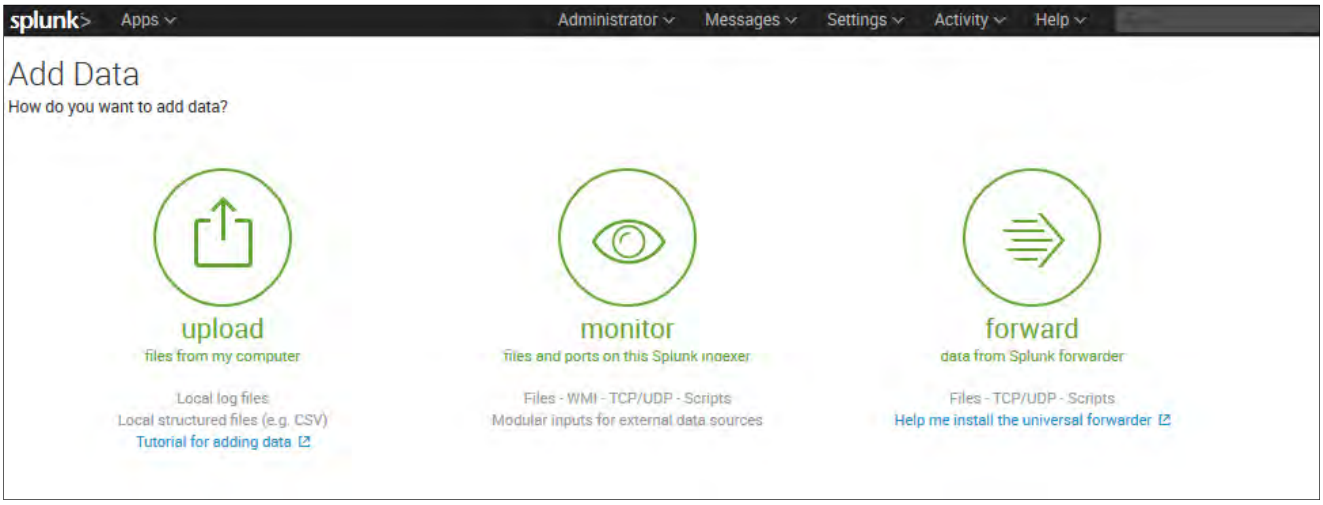
Set Up Splunk Enterprise

1. On the server where Splunk Enterprise is installed, connect to http://localhost:8000/en-US/account/login. The first time you log in, use the default user name **admin** and the default password **changeme**. You can then change the password to one you choose and log in again with your new password.

2. From Splunk Home, select **Add Data**. The **Add Data** page launches.

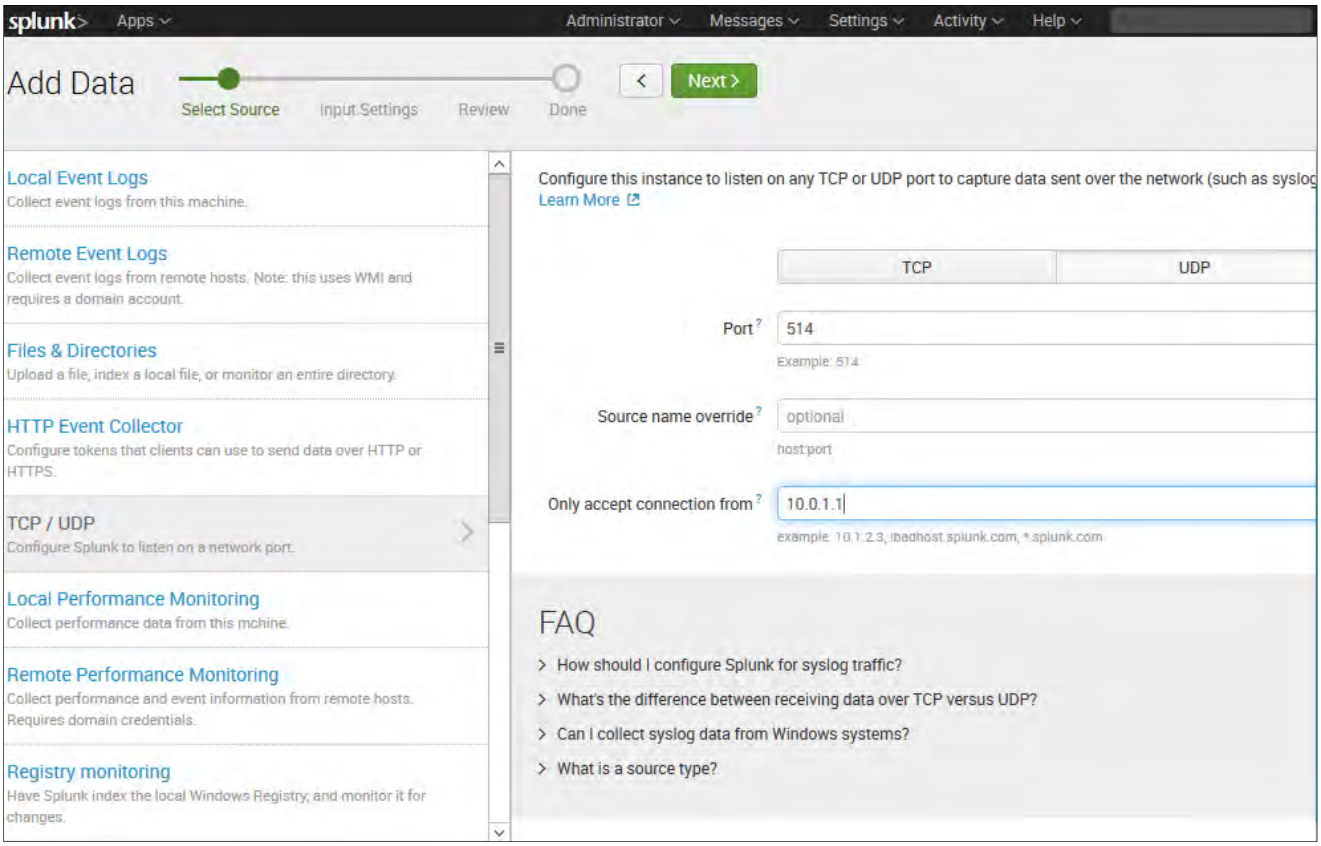


3. Select **monitor** to get data from TCP and UDP ports.

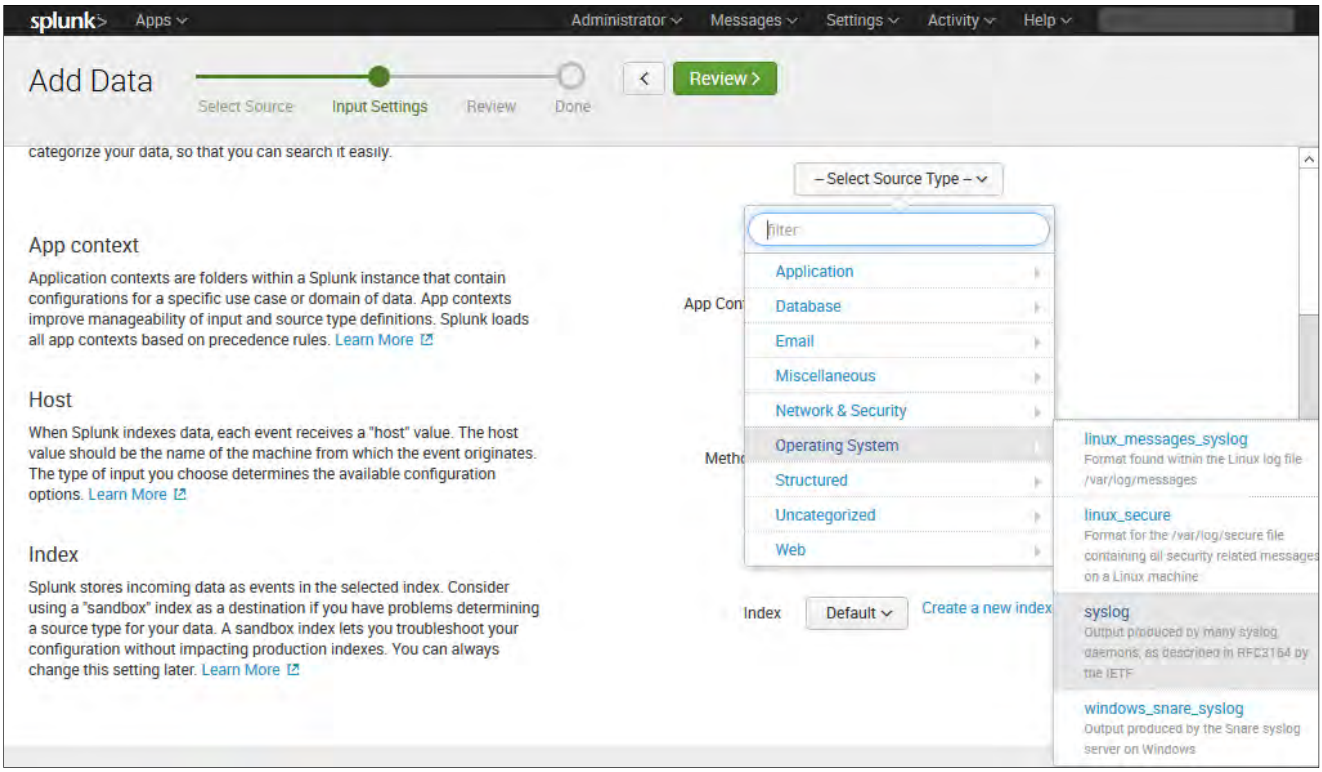


4. Select the **TCP/UDP** > **UDP** tab**.** Note that Firebox syslog support is only available for UDP.
5. In the **Port** text box, type 514. This port must match the port configured on the Firebox for the syslog server.

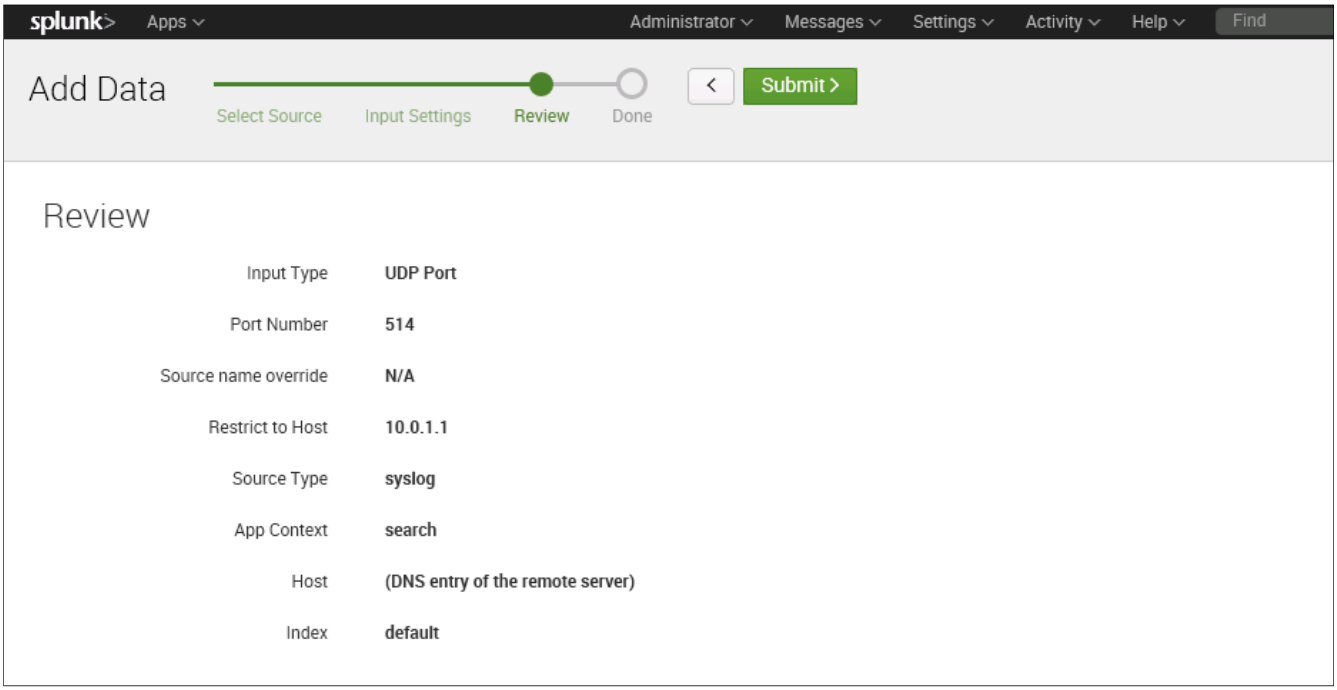
6. In the **Only accept connection from** text box, type the IP address of your Firebox. In our example, we used `10.0.1.1`.



7. From the **Select Source Type** drop-down list, select **Operating System > syslog**. Click **Review** to continue.

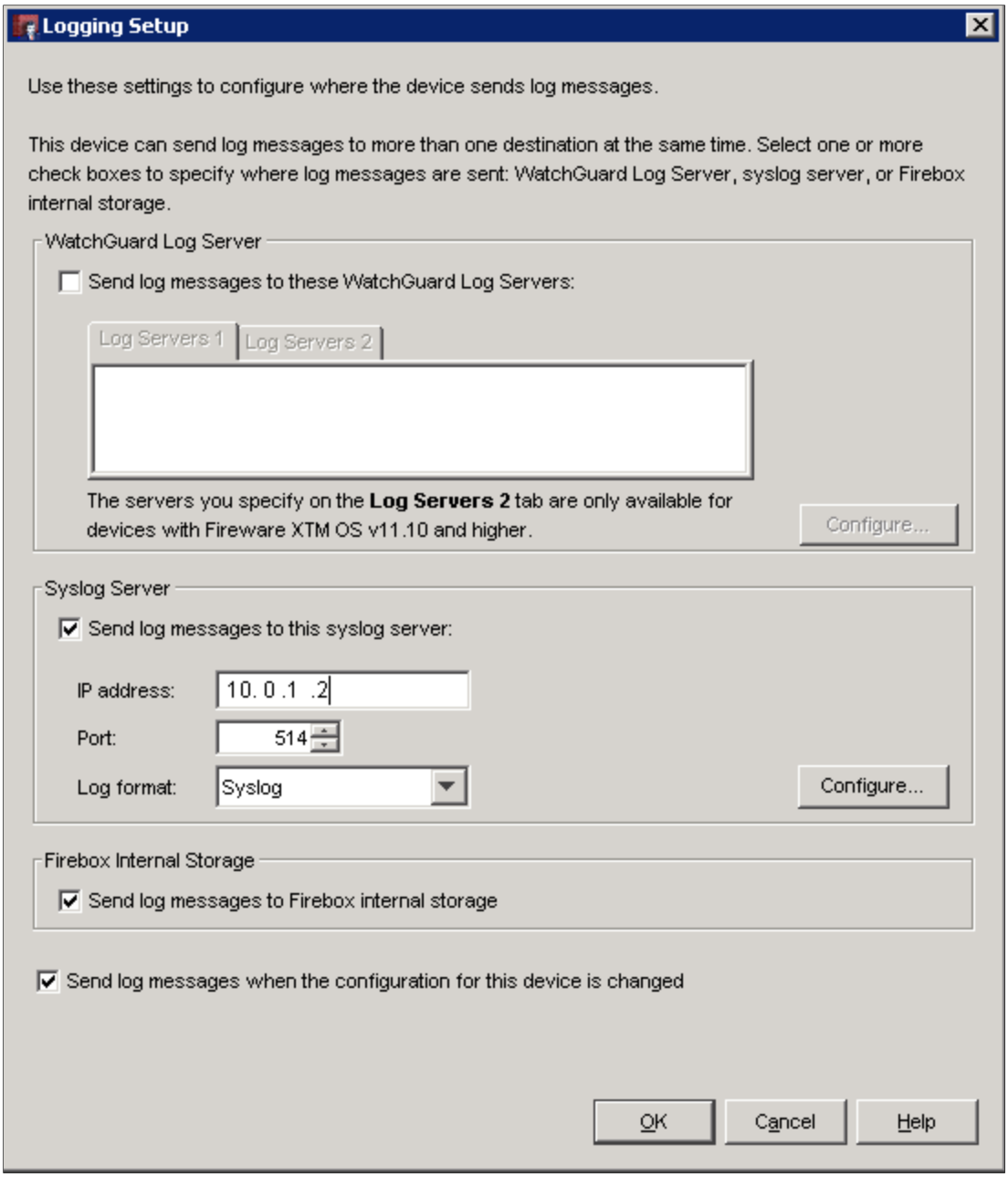


8. Click **Submit**. Splunk will now automatically receive syslog messages from the Firebox IP address you specified.



Set Up Your Firebox to Send Syslog Messages to Splunk

1. Connect to your Firebox with WatchGuard System Manager > Policy Manager or Fireware Web UI. In this example, we use Policy Manager.
2. Select **Setup > Logging**.

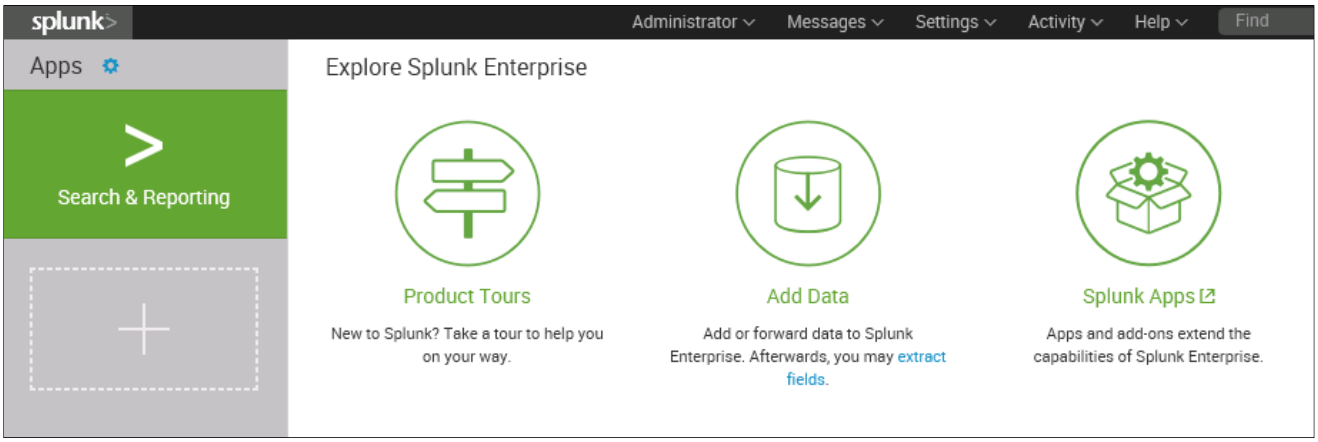


3. Select the **Send log messages to this syslog server** check box.
4. In the **IP address** text box, type the IP addrees of your server on which Splunk is installed. In this example, we use `10.0.1.2`.
5. From the Port selector, select **514.**
6. From the **Log format** drop-down list, select **Syslog**.

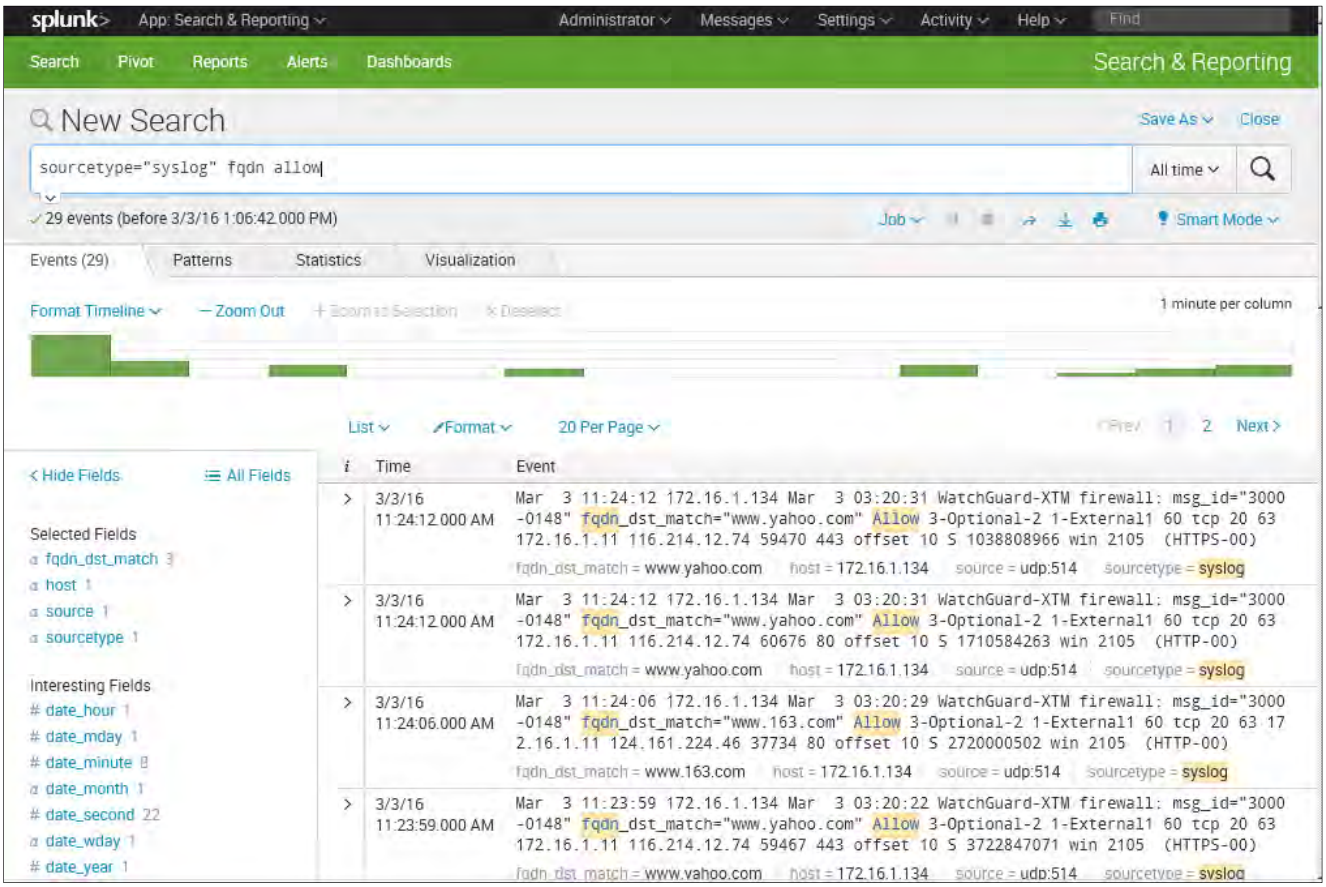
7. Click **OK**. Save the configuration to your Firebox.

Search and Report on syslog Data from Splunk

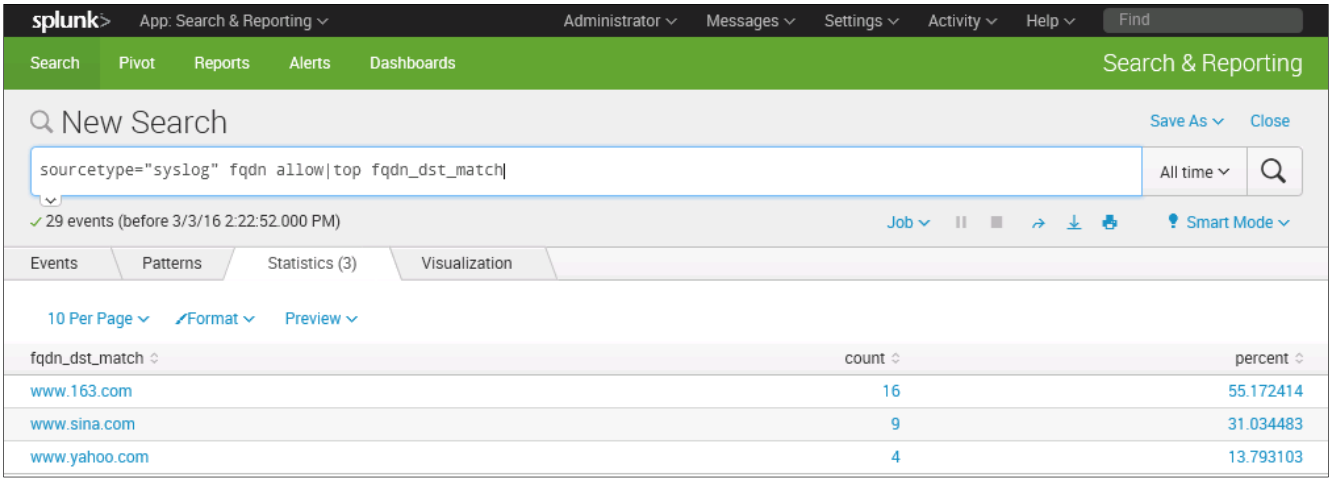
1. Sign in to the Splunk Home Page with the user **admin** and your administrative password**.**
2. Click **Search & Reporting.**



3. In the **New Search** text box, type a search command to find a log message, using Splunk's supported search language commands. For example, this screenshot shows a search for log messages related to website browsing of an internal host through the Firebox.



4. With Splunk reporting, we can count the number of times an internal host visited any website.



5. Click the **Visualization** tab to visualize the report resulting from your search. In our example, we selected to view the data as a pie chart.