Integration Guide

IBM QRadar® Security Intelligence Platform

Device Support Module (DSM)

Revised: 14 March 2016

About This Guide

Guide Type

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

Guide Details

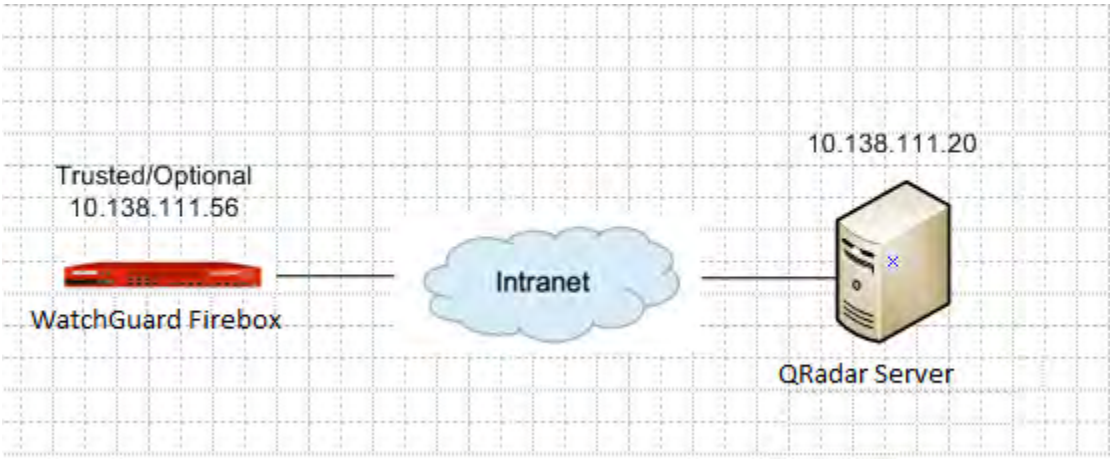
WatchGuard provides integration instructions to help our customers configure WatchGuard products to work with products created by other organizations. If you need more information or technical support about how to configure a third-party product, see the documentation and support resources for that product.

IBM Security QRadar DSM Integration Overview

IBM Security QRadar® can collect events from your WatchGuard Firebox using a plugin file called a DSM (Device Support Module).At a high level, here are the steps necessary to integration QRadar DSN with your Firebox:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - DSMCommon RPM
   - WatchGuard Fireware OS RPM
2. Configure your Firebox to enable communication with QRadar
3. If QRadar does not automatically discover the Fireware log source, create a log source for each instance of WatchGuard Fireware OS on your network.

Steps 2 and 3 are described in this document, based on the IP addresses used in this diagram:



Platform and Software

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

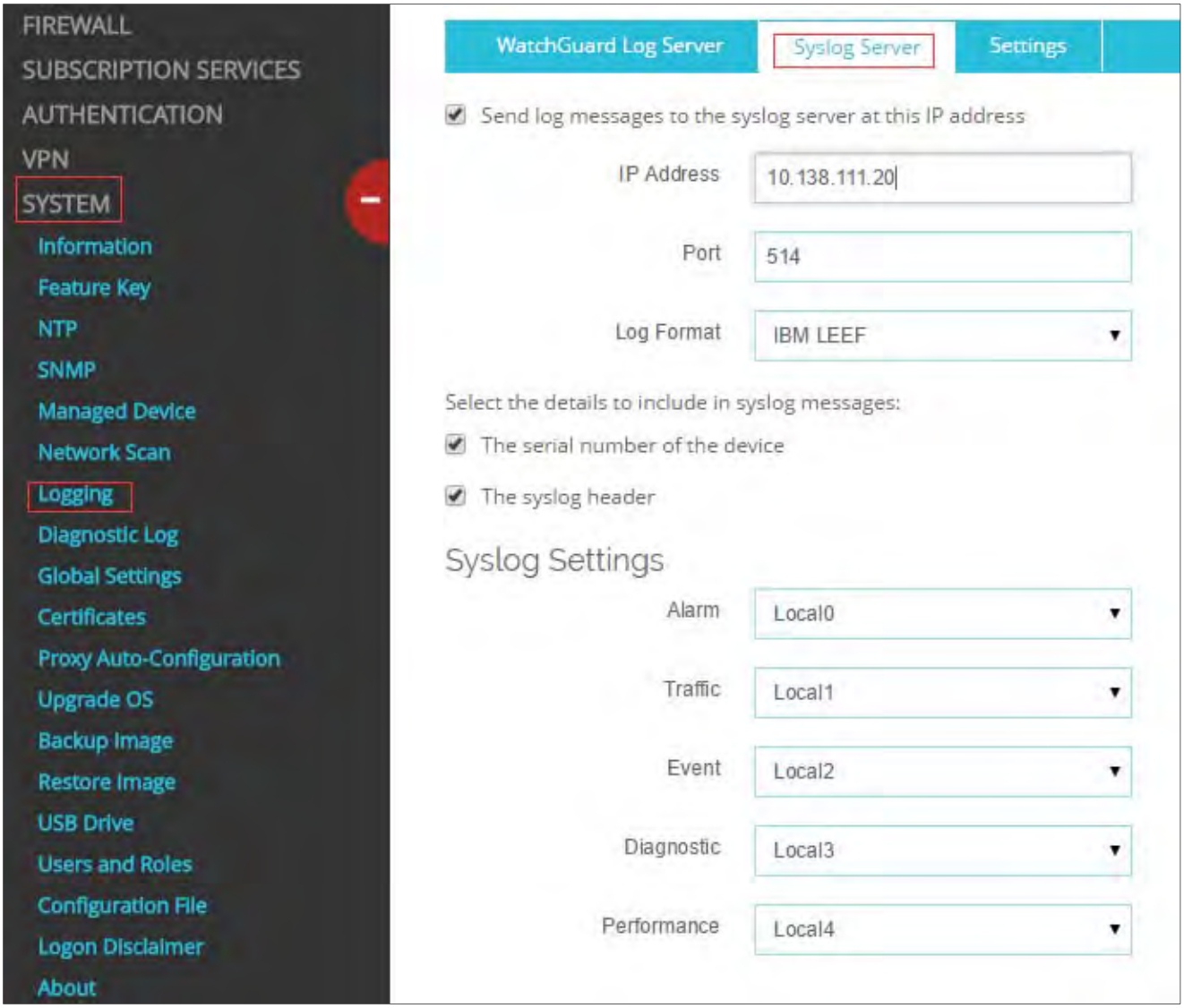
- Firebox or WatchGuard XTM device installed with Fireware v11.11 (the integration is supported with Fireware v11.9 and higher)
- DSM name: WatchGuard Fireware OS
- RPM file name :DSM-WatchGuardFirewareOS-QRadar-version-Build_number.noarch.rpm

Configure your Firebox to Communicate with QRadar

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

Note: You must have Device Administrator access credentials for the Firebox.

1. Connect to the Firebox with Fireware Web UI (https://<Firebox_IP_or_Domain_Name>:8080).
2. Select **System** > **Logging.**
3. In the **Syslog Server** pane, click the **Send log messages to the syslog server at this IP address** check box.
4. In the **IP Address** text box, type the **IP address** for the QRadar Console or Event Collector.
5. In the **Port** text box, type 514.
6. From the **Log Format** drop-down list, select **IBM® LEEF**.
7. If you want to include the serial number of the Firebox in the log message details, select this check box: **The serial number of the device**.
8. If you want to include the syslog header in the log message details, select this check box: **The syslog header**.
9. For each type of log message, select one of the following syslog facilities:
    - For high-priority syslog messages, such as **alarms**, select **Local0**.
    - To assign priorities to other types of log messages, select an option from Local1 through Local7. Lower numbers have greater priority.
    - To not send details for a log message type, select **NONE**.
10. Click **Save**.



Configure a WatchGuard Fireware OS Log Source in QRadar

Use this procedure if your QRadar Console did not automatically discover the WatchGuard Fireware OS log source.

1. Log in to QRadar
2. Click the **Admin** tab.
3. In the **Navigation** menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. In the **Log Source Identifier** field, type the **IP address** or **host name** of the WachGuard Firebox.
7. From the **Log Source Type** list, select **WatchGuard Fireware OS**.
8. From the **Protocol Configuration** list, select **Syslog**.

9. Configure the remaining parameters.
10. Click **Save**.