WatchGuard Fireware OS

The IBM® Security QRadar® DSM for WatchGuard Fireware OS can collect event logs from your WatchGuard Fireware OS.

The following table identifies the specifications for the WatchGuard Fireware OS DSM:

Table 1. WatchGuard Fireware DSM specifications

Specification	Value
Manufacturer	WatchGuard
DSM name	WatchGuard Fireware OS
RPM file name	DSM-WatchGuardFirewareOS-*QRadar-version-Build_number*.noarch.rpm
Supported versions	Fireware XTM OS v11.9 and later
Event format	syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Includes identity?	No
More information	WatchGuard Website (http://www.watchguard.com/)

To integrate the WatchGuard Fireware OS with QRadar, use the following steps:

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. For each instance of WatchGuard Fireware OS, configure your WatchGuard Fireware OS appliance to enable communication with QRadar. You can use one the following procedures:
   - "Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar"
   - "Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar" on page 2
3. If QRadar does not automatically discover the WatchGuard Fireware OS log source, create a log source for each instance of WatchGuard Fireware OS on your network.

Configuring your WatchGuard Fireware OS appliance in Policy Manager for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Policy Manager to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Open the WatchGuard System Manager.
2. Connect to your Firebox or XTM device.
3. Start the Policy Manager for your device.
4. To open the Logging Setup window, select **Setup > Logging**.
5. Select the **Send log messages to this syslog server** check box.
6. In the **IP address** text box, type the IP address for your QRadar Console or Event Collector.
7. In the **Port** text box, type 514.
8. From the **Log Format** list, select **IBM LEEF**.
9. Optional: Specify the details to include in the log messages.
   a. Click **Configure**.
   b. To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.
   c. To include the syslog header in the log message details, select the **The syslog header** check box.
   d. 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**.
   e. Click **OK**.
10. Click **OK**.
11. Save the configuration file to your device.

Configuring your WatchGuard Fireware OS appliance in Fireware XTM for communication with QRadar

To collect WatchGuard Fireware OS events, you can use the Fireware XTM web user interface to configure your third-party appliance to send events to QRadar.

Before you begin

You must have Device Administrator access credentials.

Procedure

1. Log in to the Fireware XTM web user interface for your Fireware or XTM device.
2. Select **System > Logging**.
3. In the Syslog Server pane, select 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** list, select **IBM LEEF**.
7. Optional: Specify the details to include in the log messages.
   a. To include the serial number of the XTM device in the log message details, select the **The serial number of the device** check box.

b. To include the syslog header in the log message details, select the **The syslog header** check box.

c. 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**.

8. Click **Save**.

Configuring 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.

Procedure

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 WatchGuard Fireware OS device.
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**.