IBM Security Network IPS

The IBM Security Network IPS DSM for IBM Security QRadar® collects LEEF-based events from IBM Security Network IPS appliances by using the syslog protocol.

The following table identifies the specifications for the IBM Security Network IPS DSM:

Parameter	**Value**
Manufacturer	IBM
DSM	Security Network IPS
RPM file name	DSM-IBMSecurityNetworkIPS-*QRadar_version-Build_number*.noarch.rpm
Supported versions	v4.6 and later (UDP) v4.6.2 and later (TCP)
Protocol	syslog (LEEF)
QRadar recorded events	Security alerts (including IPS and SNORT) Health alerts System alerts IPS events (Includubg security, connection, user defined, and OpenSignature policy events)
Automatically discovered?	Yes
Includes identity?	No

To integrate the IBM Security Network IPS appliance with QRadar, use the following steps:

1. If automatic updates are not enabled, download and install the most recent version of the IBM Security Network IPS RPMs on your QRadar Console.
2. For each instance of IBM Security Network IPS, configure your IBM Security Network IPS appliance to enable communication with QRadar.
3. If QRadar does not automatically discover the log source, create a log source for each instance of IBM Security Network IPS on your network.

Configuring your IBM Security Network IPS appliance for communication with QRadar

To collect events with QRadar, you must configure your IBM Security Network IPS appliance to enable syslog forwarding of LEEF events.

Before you begin

Ensure that no firewall rules block the communication between your IBM Security Network IPS appliance and QRadar.

Procedure

1. Log in to your IPS Local Management Interface.
2. From the navigation menu, select **Manage System Settings** > **Appliance** > **LEEF Log Forwarding**.
3. Select the **Enable Local Log** check box.
4. In the **Maximum File Size** field, configure the maximum file size for your LEEF log file.
5. From the Remote Syslog Servers pane, select the **Enable** check box.
6. In the **Syslog Server IP/Host** field, type the IP address of your QRadar Console or Event Collector.
7. In the **TCP Port** field, type `514` as the port for forwarding LEEF log events.

   Note: If you use v4.6.1 or earlier, use the **UDP Port** field.
8. From the event type list, enable any event types that are forwarded to QRadar.
9. If you use a TCP port, configure the **`crm.leef.fullavp`** tuning parameter:
   a. From the navigation menu, select **Manage System Settings** > **Appliance** > **Tuning Parameters**.
   b. Click **Add Tuning Parameters**.
   c. In the **Name** field, type `crm.leef.fullavp`.
   d. In the **Value** field, type `true`.
   e. Click **OK**.

Configuring an IBM Security Network IPS log source in QRadar

QRadar automatically discovers and creates a log source for syslog events from IBM Security Network IPS appliances. However, you can manually create a log source for QRadar to receive syslog events.

About this task

Procedure

1. Click the **Admin** tab.
2. Click the **Log Sources** icon.
3. Click **Add**.
4. In the **Log Source Name** field, type a name for your log source.
5. From the **Log Source Type** list, select **IBM Security Network IPS (GX)**.
6. Using the **Protocol Configuration** list, select **Syslog**.
7. Configure the parameters:

Parameter	Description
Log Source Identifier	The IP address or host name for the log source as an identifier for events from your IBM Security Network IPS appliance.
Credibility	The credibility indicates the integrity of an event or offense as determined by the credibility rating from the source devices. Credibility increases if multiple sources report the same event.
Coalescing Events	Enables the log source to coalesce (bundle) events.

Parameter	Description
Incoming Event Payload	The incoming payload encoder for parsing and storing the logs.

8. Click **Save**.
9. On the **Admin** tab, click **Deploy Changes**.