TECHNICAL NOTE

CONFIGURING IPFIX

JUNE 2012

Internet Protocol Flow Information Export (IPFIX) is an accounting technology that monitors traffic flows through a switch or router, interprets the client, server, protocol, and port used, counts the number of bytes and packets, and sends that data to a IPFIX collector. IBM Security Network Protection XGS 5000, a next generation IPS, is an example of a device that sends flow traffic in IPFIX flow format.

The process of sending IPFIX data is often referred to as a NetFlow Data Export (NDE). IPFIX provides more flow information and deeper insight than NetFlow v9. You can configure QRadar to accept NDE's and thus become an IPFIX collector. IPFIX uses User Datagram Protocol (UDP) to deliver NDEs. After a NDE is sent from the IPFIX forwarding device, the IPFIX record may be purged.

This technical note includes the following topics:

- **Before you Begin**
- **Configuring IPFIX**

Before you Begin

When you configure an external flow source for IPFIX, you must:

- Ensure the appropriate firewall rules are configured. If you change your **External Flow Source Monitoring Port** parameter in the QFlow Collector configuration, you must also update your firewall access configuration. For more information on QFlow Collector configuration, see the *QRadar Administration Guide*.
- Ensure the appropriate ports are configured for your QFlow Collector.
- Ensure the IPFIX template from the IPFIX source includes the following fields:
  - FIRST_SWITCHED
  - LAST_SWITCHED
  - PROTOCOL
  - IPV4_SRC_ADDR
  - IPV4_DST_ADDR
  - L4_SRC_PORT

- L4_DST_PORT
- IN_BYTES or OUT_BYTES
- IN_PKTS or OUT_PKTS
- TCP_FLAGS (TCP flows only)

Configuring IPFIX

To configure QRadar to accept IPFIX flow traffic, you must add a NetFlow flow source. The NetFlow flow source processes IPFIX flows using the same process.

NOTE

Your QRadar system may include a default NetFlow flow source; therefore, you may not be required to perform this procedure. To confirm that your system includes a default NetFlow flow source, select **Admin > Flow Sources**. If **default_Netflow** is listed in the flow source list, IPFIX is already configured.

To add a NetFlow flow source:

Step 1 Click the **Admin** tab.

Step 2 On the navigation menu, click **Data Sources**.

The Data Sources pane is displayed.

Step 3 On the navigation menu, click **Flows**.

The Flows pane is displayed.

Step 4 Click the **Flow Sources** icon.

The Flow Sources window is displayed.

Step 5 Click **Add**.

The Add Flow Source window is displayed.

Step 6 Enter values for the parameters:

Table 1-1 Add Flow Source Window Parameters

Parameter	Description
Build from existing flow source	Select this check box if you want to create this flow source using an existing flow source as a template. After you select the check box, use the list box to select a flow source and click **Use as Template**.
Flow Source Name	Type a name for the flow source. We recommend that for an external flow source that is also a physical device, you use the device name as the flow source name. If the flow source is not a physical device, ensure you use a an appropriate and recognizable name. For example, if you want to use IPFIX traffic, type **`nf1`**.
Target Collector	Using the list box, select the Event Collector you want to use for this flow source.
Flow Source Type	From the list box, select the **Netflow v.1, v5, v7, or v9** option.

Table 1-1 Add Flow Source Window Parameters (continued)

Parameter	Description
Enable Asymmetric Flows	In some networks, traffic is configured to take alternate paths for inbound and outbound traffic. This is asymmetric routing. Select this check box if you want to enable asymmetric flows for this flow source.
Monitoring Interface	Using the list box, select the monitoring interface you want to use for this flow source.
Source File Path	Type the source file path for the flowlog file.
Monitoring Port	Type the monitoring port you want this flow source to use. For the first NetFlow flow source configured in your network, the default port is 2055. For each additional NetFlow flow source, the default port number increments by 1. For example, the default NetFlow flow source for the second NetFlow flow source is 2055.
Enable Flow Forwarding	Select this check box to enable flow forwarding for this flow source. When you select the check box, the following options are displayed: • **Forwarding Port** - Type the port you want to forward flows. The default is 1025. • **Forwarding Destinations** - Type the destinations you want to forward flows to. You can add or remove addresses from the list using the **Add** and **Remove** icons.

Step 7 Click **Save**.

Step 8 On the **Admin** tab menu, click **Deploy Changes**.

Q1 Labs Inc.
890 Winter Street
Suite 230
Waltham, MA 02451 USA