92 SOURCEFIRE

IBM Security QRadar supports the following Sourcefire devices:

- **Sourcefire Defense Center (DC)**
- **Sourcefire Intrusion Sensor**

Sourcefire Defense Center (DC)

The IBM Security QRadar DSM for Sourcefire Defense Center accepts Sourcefire Defense Center events using the eStreamer API service.

Supported versions

QRadar supports the following versions of Sourcefire Defense Center:

- Sourcefire Defense Center v4.8.2.x and later
- Sourcefire Defense Center v5.x

  You must download and install one of the following hotfixes from the Sourcefire website to collect Sourcefire Defense Center 5.x events in QRadar:

  - Sourcfire_hotfix-v5.1.0-0-build_1.tar
  - Sourcfire_hotfix-v5.1.1-0-build_1.tar

  For more information on hotfixes for your Sourcefire appliance, see the Sourcefire website.

Configuration overview

To integrate with Sourcefire Defense Center, you must create certificates in the Sourcefire Defense Center interface, and then add the certificates to the QRadar appliances that receive eStreamer event data.

If your deployment includes multiple Sourcefire Defense Center appliances, you must copy the certificate for each appliance that receives eStreamer events. The certificate allows the Sourcefire Defense Center appliance and the QRadar Console or Event Collector to communicate by using the eStreamer API to collect events.

To integrate QRadar with Sourcefire Defense Center, use the following steps:

1. Create the eStreamer certificate on your Sourcefire Defense Center appliance.
2. Add the Sourcefire Defense Center certificate files to QRadar.
3. Configure a log source in QRadar for your Sourcefire Defense Center appliances.

Supported event types

QRadar supports the following event types from Sourcefire Defense Center:

- Intrusion events and extra data

  Intrusion events categorized by the Sourcefire Defense Center DSM in QRadar use the same QRadar Identifiers (QIDs) as the Snort DSM. To ensure that all intrusion events are categorized properly, you can download and install the latest Snort DSM from *http://www.ibm.com/support.*

  Intrusion events in the 1,000,000 to 2,000,000 range are user-defined rules in Sourcefire Defense Center. User-defined rules that generate events are added as an Unknown event in QRadar, and include additional information describing the event type. For example, a user-defined event can identify as Unknown:Buffer Overflow for Sourcefire Defense Center.
- Correlation events
- Metadata events
- Discovery events
- Host events
- User events

Creating Sourcefire 4.x certificates

QRadar requires a certificate for every Sourcefire Defense Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to keystore and truststore files, which are usable by QRadar appliances.

Procedure

Step 1 Log in to your Sourcefire Defense Center interface.

Step 2 Select **Operations > Configuration > eStreamer**.

Step 3 Click the **eStreamer** tab.

Step 4 Click **Create Client**.

Step 5 Select check boxes for the event types Sourcefire Defense Center provides to QRadar.

Step 6 Click **+ Create Client** located in the upper right-side of the interface.

Step 7 In the **Hostname** field, type the IP address or host name.

- If you use a QRadar Console or use an All-in-one appliance to collect eStreamer events, type the IP address or host name of your QRadar Console.
- If you use a remote Event Collector to collect eStreamer events, type the IP address or host name for the remote Event Collector.

- If you use High Availability (HA), type the virtual IP address.

Step 8 In the **Password** field, leave the password field blank or type a password for your certificate.

Step 9 Click **Save**.

The new client is added to the Streamer Client list and the host is allowed to communicate with the eStreamer API on port 8302.

Step 10 From the **Certificate Location** column, click the client you created to save the pkcs12 certificate to a file location and click **OK**.

You are now ready to import your Sourcefire Defense Center certificate to your QRadar appliance.

Creating Sourcefire 5.x certificates

Certificates are created by Sourcefire Defense Center appliances in your deployment.

QRadar requires a certificate for every Sourcefire Defense Center appliance in your deployment. Certificates are generated in pkcs12 format and must be converted to a keystore and truststore file, which are usable by QRadar appliances.

Procedure

Step 1 Log in to your Sourcefire Defense Center interface.

Step 2 Select **System > Local > Registration**.

Step 3 Click the **eStreamer** tab.

Step 4 Select check boxes for the event types Sourcefire Defense Center provides to QRadar.

WARNING: *For Sourcefire Defense Center 5.x, you must clear the* ***Impact Flag Alerts*** *check box.*

Step 5 Click **Save**.

Step 6 Click **+ Create Client** located in the upper right-side of the interface.

Step 7 In the **Hostname** field, type the IP address or hostname.

- If you use QRadar Console or use an All-in-one appliance to collect eStreamer events, type the IP address or hostn ame of your QRadar Console.
- If you use an Event Collector to collect eStreamer events, type the IP address or hostname for the Event Collector.
- If you use High Availability (HA), type the virtual IP address.

Step 8 In the **Password** field, type a password for your certificate or leave the field blank.

Step 9 Click **Save**.

The new client is added to the Streamer Client list and the host is allowed to communicate with the eStreamer API on port 8302.

Step 10 Click the download arrow for your host to save the pkcs12 certificate to a file location.

Step 11 Click **OK** to download the file.

You are now ready to import your Sourcefire Defense Center certificate to your QRadar appliance.

Importing a certificate to QRadar

The estreamer-cert-import.pl script for QRadar converts your pkcs12 certificate file to a keystore and truststore file and places the certificates in the proper directory on your QRadar appliance. Repeat this procedure for each Sourcefire Defense Center pcks12 certificate you need to import to your QRadar Console or Event Collector.

Before you begin

You must have root or su - root privileges to run the estreamer-cert-import.pl import script.

About this task

The estreamer-cert-import.pl script is stored on your QRadar appliance when you install the Sourcefire Defense Center protocol.

The script converts and imports one pkcs12 file at a time. You are required only to import a certificate for the QRadar appliance that manages the Sourcefire Defense Center log source. For example, after the Sourcfire event is categorized and normalized by an Event Collector in a QRadar distributed deployment, it is forwarded to the QRadar Console. In this scenario, you would import a certificate to the Event Collector.

When you import a new certificate, existing Sourcefire Defense Center certificates on the QRadar appliance are renamed to estreamer.keystore.old and estreamer.truststore.old.

Procedure

Step 1 Using SSH, log in to your QRadar Console or Event Collector as the root user.

Step 2 Copy the pkcs12 certificate from your Sourcefire Defense Center appliance to the following directory in QRadar:

`/opt/qradar/bin/`

Step 3 To import your pkcs12 file, type the following command and any extra parameters:

`/opt/qradar/bin/estreamer-cert-import.pl -f` ***`pkcs12_file_name options`***

Extra parameters are described in the following table:

Table 92-1 Sourcefire Defense Center Import Script Parameters

Parameter	Description
-f	The -f parameter identifies the file name of the pkcs12 files to import. This parameter is required to import certificates.

Table 92-1 Sourcefire Defense Center Import Script Parameters (continued)

Parameter	Description
-o	Overrides the default estreamer name for the keystore and truststore files. The -o parameter is required when using multiple Sourcefire Defense Center devices, as unique key file names are required. For example, **/opt/qradar/bin/estreamer-cert-import.pl -f <file name> -o 192.168.1.100** The import script creates the following files: /opt/qradar/conf/192.168.0.100.keystore /opt/qradar/conf/192.168.0.100.truststore
-d	Enables verbose mode when using the import script. Verbose mode is intended to display error messages for troubleshooting purposes when pkcs12 files fail to import properly.
-p	Specifies a password if a password was accidently provided when generating the pkcs12 file.
-v	Displays the version information for the import script.
-h	Displays a help message on using the import script.

For example,

/opt/qradar/bin/estreamer-cert-import.pl -f 192.168.0.1.pkcs12

Result

The import script creates a keystore and truststore file in the following locations:

```
/opt/qradar/conf/estreamer.keystore
/opt/qradar/conf/estreamer.truststore
```

Configure a log source

You must configure a log source because QRadar does not automatically discover Sourcefire Defense Center events.

Procedure

Step 1 Log in to QRadar.

Step 2 Click the **Admin** tab.

Step 3 On the navigation menu, click **Data Sources**.

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

Step 5 Click **Add**.

Step 6 From the **Log Source Type** list, select **Sourcefire Defense Center**.

Step 7 From the **Protocol Configuration** list, select **Sourcefire Defense Center Estreamer**.

Step 8 Configure the following parameters:

Table 92-2 Sourcefire Defense Center Estreamer Parameters

Parameter	Description
Server Address	The IP address or hostname of the Sourcefire Defense Center device.
Server Port	The port number QRadar uses to receive Sourcefire Defense Center Estreamer events. The default is 8302.
Keystore Filename	The directory path and file name for the keystore private key and associated certificate.
Truststore Filename	The directory path and file name for the truststore files. The truststore file contain the certificates trusted by the client.
Request Extra Data	Select this option to request extra data from Sourcefire Defense Center Estreamer, for example, extra data includes the original IP address of an event.

Sourcefire Intrusion Sensor

The Sourcefire Intrusion Sensor DSM for IBM Security QRadar accepts Snort based intrusion and prevention syslog events from Sourcefire devices.

Configuring Sourcefire Intrusion Sensor

To configure your Sourcefire Intrusion Sensor, you must enable policy alerts and configure your appliance to forward the event to QRadar.

Procedure

Step 1 Log in to your Sourcefire user interface.

Step 2 On the navigation menu, select **Intrusion Sensor > Detection Policy > Edit**.

Step 3 Select an active policy and click **Edit**.

Step 4 Click **Alerting**.

Step 5 In the **State** field, select **on** to enable the syslog alert for your policy.

Step 6 From the **Facility** list, select **Alert**.

Step 7 From the **Priority** list, select **Alert**.

Step 8 In the **Logging Host** field, type the IP address of the QRadar Console or Event Collector.

Step 9 Click **Save**.

Step 10 On the navigation menu, select **Intrusion Sensor > Detection Policy > Apply**.

Step 11 Click **Apply**.

You are now ready to configure the log source in QRadar.

Configuring a log source in QRadar

QRadar automatically discovers and creates a log source for syslog events from Sourcefire Intrusion Sensor. However, you can manually create a log source for QRadar to receive syslog events. The following procedure is optional.

Procedure

Step 1 Log in to QRadar.

Step 2 Click the **Admin** tab.

Step 3 On the navigation menu, click **Data Sources**.

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

Step 5 Click **Add**.

Step 6 In the **Log Source Name** field, type a name for your log source.

Step 7 In the **Log Source Description** field, type a description for the log source.

Step 8 From the **Log Source Type** list, select **Snort Open Source IDS**.

Step 9 Using the **Protocol Configuration** list, select **Syslog**.

Step 10 Configure the following values:

Table 92-3 Syslog Parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for events from your Sourcefire Intrusion Sensor appliance.

Step 11 Click **Save**.

Step 12 On the **Admin** tab, click **Deploy Changes**.

The configuration is complete.