RSA NetWitness Logs

Event Source Log Configuration Guide

Proofpoint Email Security

Last Modified: Friday, June 02, 2017

Event Source Product Information:

Vendor: Proofpoint
Event Source: Email Security
Versions: 6.3, 7.2, 7.5, 8.x

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: proofpoint
Collection Method: Syslog
Event Source Class.Subclass: Security.Application Firewall

Configure Proofpoint Email Security

To configure Syslog collection for the Proofpoint Email Security event source, perform the following tasks:

I. Configure Syslog Output on Proofpoint, depending on your version:

- Configure Proofpoint Version 7.2 and later, or
- Configure Proofpoint Version 6.3.

II. Configure RSA NetWitness Suite for Syslog Collection

Configure Proofpoint Version 7.2 and Later

Follow these instructions if you are using Proofpoint version 7.2 or later.

To configure Proofpoint version 7.2 or later to work with RSA NetWitness Suite, follow these steps:

1. Log on to the Proofpoint Email Security web interface with administrative credentials.
2. Click **Logs and Reports** > **Log Settings**.
3. In the **Remote Log Options** section, update the following settings:

Field	Action
Syslog Protocol	Select **UDP**.
Syslog Host	Enter the IP address of your RSA NetWitness Suite Log Decoder or Remote Log Collector
Syslog Port	Ensure this is set to **514**.
Syslog Filter Enable	Set to **On** to receive security-related events.
Syslog MTA Enable	Set to **On** to receive mail events.

4. Click **Save Changes**.

Configure Proofpoint Version 6.3

Follow these instructions if you are using Proofpoint version 6.3.

To configure Proofpoint version 6.3 to work with RSA NetWitness Suite, follow these steps:

1. Log on to the Proofpoint Email Security web interface with administrative credentials.
2. You must switch to Advanced Mode. To switch modes, in the top right corner, click **Switch to Advanced Mode**.
3. Click **Logs and Reports** > **Log Settings**.
4. In the **Log Options** section, set the settings as follows:

Field	Action
Log File Level	From the drop-down list, select your desired log file level.
Retain Log File For	Enter the amount of days that your want to retain log files.
Syslog Enable	To ensure that syslog collection is enabled, select **On**.
Syslog Level	From the drop-down list, select your desired syslog level.
Syslog Facility	From the drop-down list, select **local0**.
Syslog Host	Enter the IP address of your NetWitness Suite Log Decoder or Remote Log Collector

5. Click **Save Changes**.

Configure RSA NetWitness Suite

Perform the following steps in Security Analytics:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Suite Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.

3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

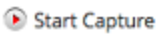
Note: The required parser is **proofpoint**.

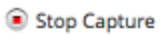
Configure Syslog Collection

Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:
   - If you see 

, click the icon to start capturing Syslog.
   - If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.

7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks