RSA NetWitness Logs

Event Source Log Configuration Guide

McAfee Firewall Enterprise

Last Modified: Wednesday, February 15, 2017

Event Source Product Information:

Vendor: McAfee
Event Source: Firewall Enterprise (formerly Secure Computing Sidewinder G2 Security Appliance)
Versions: 6.1.1.x, 6.1.2.x, 7.0.0.x, 8.x

RSA Product Information:

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

To configure the McAfee Firewall Enterprise event source, you must:

I. Configure Syslog Output on McAfee Firewall Enterprise. Depending on your version of McAfee Firewall Enterprise, do one of the following tasks:

- Configure Sidewinder G2 Security Appliance 7.0 and earlier
- Configure McAfee Firewall Enterprise 8.0 and 8.2

II. Configure RSA NetWitness Suite for Syslog Collection

Configure McAfee Firewall Enterprise 8.0 and 8.2

To configure McAfee Firewall Enterprise:

1. Log on to the McAfee Firewall Enterprise console and connect to the firewall that you want to configure.
2. In the file tree, click *Firewall Name* > **Monitor** > **Audit Management**.
3. On the **Firewall Reporter/Syslog** tab, in the **Export audit to syslog servers** section, follow these steps:
   a. Click the + button.
   b. In the new row, enter the following information:

Column	Action
IP Address	Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
Remote Facility	Leave the default value **local0**.
Description	(Optional) Enter a description.

4. Click the save button.

Configure Sidewinder G2 Security Appliance 7.0 and earlier

To configure Sidewinder:

1. Log on to the Sidewinder appliance.
2. To configure Sidewinder to send syslog messages, do the following:
   a. Use a text editor to open the file **/etc/sidewinder/auditd.conf**.

   b. Search for the **filebegin_rules** section and locate the following lines:

   ```
   log(logfile filters[] type)
   syslog(facility filters[] format)
   ipaddr_resolution(src_addr dst_addr)
   time_format(zone)
   end_rules
   ```

   Note: If the **filebegin_rules** section does not display in your search, type the lines listed in this step into the file.

   c. After the lines listed in step b, type the following:

   ```
   syslog(local0 filters["NULL"] sef)
   ```

   d. Save and close the file.
3. To configure Sidewinder to send syslog messages to RSA NetWitness Suite, follow these steps:
   a. Use a text editor to open the file **/etc/syslog.conf**.

   b. Type the following line:

   ```
   local0.*    @IP_address_<Platform>
   ```

   where *IP_address_<Platform>* is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

   Note: If you wish to send a syslog to two different IP addresses, enter two "local0" entries:

   ```
   local0.*      @IP_address_of_your_<Platform1>
   local0.*      @IP_address_of_your_<Platform2>
   ```

   c. Save and close the file.

4. To restart the **auditd** and **syslogd** services, do the following:

   a. Enter the following command to go to the administrator domain:

      ```
      srole
      ```

   b. Depending on your version of Sidewinder, type the following commands to restart the services:

      - For Sidewinder versions 7.0.0 and later, type:

        ```
        cf daemond restart agent=syslog
        cf daemond restart agent=auditd
        ```

      - For Sidewinder versions prior to 7.0.0, type:

        ```
        kill -HUP syslogpid
        cf server restart auditd
        ```

Configure NetWitness Suite

Perform the following steps in RSA NetWitness Suite:

- 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 **sidewinder**.

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 ● Start Capture , click the icon to start capturing Syslog.
- If you see ● Stop Capture , 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