RSA NetWitness Platform

Event Source Log Configuration Guide

Fortinet FortiGate

Last Modified: Friday, May 3, 2019

Event Source Product Information:

Vendor: Fortinet
Event Source: FortiGate
Versions: FortiOS v 2.8, 3.0, 4.0 MR1, 4.0 MR2, 5.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

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

To configure the Fortinet FortiGate event source, you must:

I. Configure Syslog Output on Fortinet FortiGate

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Fortinet FortiGate

Configure your version of FortiGate:

- Configure Fortinet FortiGate 5.x
- Configure Fortinet FortiGate 4.0 MR1 or 4.0 MR2
- Configure Fortinet FortiGate 3.0
- Configure Fortinet FortiGate 2.8

Configure Fortinet FortiGate 5.x

To enable logging to the Syslog server:

Log into the FortiGate Command Line Interface as Administrator and enter the following commands:

```
config log syslogd setting
set status enable
set server NW-IP-address
set csv disable
set facility facility-name
end
```

Where:

- ***NW-IP-address*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector
- ***facility-name*** is a name of your choice

> **Note:** For the facility option, RSA supports local0, local1, and so on.

Configure Fortinet FortiGate 4.0 MR1 or 4.0 MR2

To configure logging for version 4.0 MR1 or 4.0 MR2, you must complete these tasks:

> **Note:** If you are using FortiGate 4.0 MR2. you must enable logging for each component and only complete task III.

I. Configure firewall policy logging

II. Configure protection profile logging

III. Configure log settings

Configure Firewall Policy Logging

1. Click **Firewall** > **Policy**.
2. Edit each policy by selecting **Log Allowed Traffic**.
3. Click **OK**.

Configure Protection Profile Logging

1. Click **Firewall** > **Protection Profile**.
2. For the protection profile that you want to use, select **Edit**.
3. Click the blue arrow next to **Logging**, and select the features that you want to log.
4. Click **OK**.

Configure Log Setting

1. Click **Log&Report > Log Config > Log Setting**.
2. Select **Remote Logging and Archiving**.
3. Select **Syslog**, and follow these steps:
   a. Enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   b. In the port number field, type **514**.
   c. Select any logging severity level except **Debug**.
   d. Select the log facility.
   e. Make sure the **Enable CSV format** option is not selected.
4. Click **Apply**.

Configure Fortinet FortiGate 3.0

To configure logging for version 3.0, you must complete these tasks:

I. Enable traffic logging per interface.

II. Configure firewall policy logging.

III. Configure protection profile logging.

IV. Configure log settings.

Enable Traffic Logging

1. Click **System > Network > Interface**.
2. Select the **Edit** icon for an interface.
3. Select **Log**.
4. Click **OK**.
5. Repeat steps 1 though 4 for each interface for which you want to enable logging.

Configure Firewall Policy Logging

1. Click **Firewall > Policy**.
2. Edit each policy by selecting **Log Allowed Traffic**.

Configure Protection Profile Logging

1. Click **Firewall > Protection Profile**.
2. For the protection profile that you want to use, select **Edit**.
3. Click the blue arrow next to **Logging**, and select all necessary settings.

Configure Log Setting

1. Click **Log&Report > Log Config > Log Setting**.
2. Select the locations to which you want to log.
3. Select the blue arrow next to the location, and follow these steps:
   a. If you are logging to a remote location, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   b. If you are logging to a remote syslog server, in the port number field, type **514**.
   c. Select the logging severity level.

d. Select the log facility.

e. If you are logging to the local disk, configure the log roll settings.

f. Make sure the **Enable CSV format** option is not selected.

4. Repeat step 3 to configure additional logging locations.
5. Click **Apply**.

Configure Fortinet FortiGate 2.8

To configure logging for version 2.8, you must complete these tasks:

I. Enable traffic logging.

II. Configure log settings.

Enable Traffic Logging

You can enable traffic logging for an interface or VLAN subinterface (if available). All connections to and through the interface are recorded in the traffic log.

To enable traffic logging:

1. Click **System > Network > Interface**.
2. Select the **Edit** icon for an interface.
3. Select **Log**.
4. Click **OK**.
5. Repeat steps 1 though 4 for each interface for which you want to enable logging.

Configure Log Settings

Log setting configuration is organized by log location. Configure log settings for each location to which you want to record logs. If you want to log traffic, you must also enable traffic logging for specific interfaces and firewall policies.

To configure log setting:

1. Click **Log&Report > Log Config > Log Setting**.
2. Select the locations to which you want to log..
3. Select the blue arrow next to the location, and follow these steps:

a. If you are logging to a remote location, enter the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

b. If you are logging to a remote syslog server, in the port number field, type **514**.

c. Select the logging severity level.

d. If you are logging to the local disk, configure the log roll settings.

e. Make sure the **Enable CSV format** option is not selected.

4. Repeat step 3 to configure additional logging locations.

5. Click **Apply**.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- 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 Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **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 **fortinet**.

Configure Syslog Collection

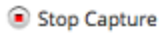
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.