

RSA NetWitness Logs

Event Source Log Configuration Guide



F5 Big-IP Advanced Firewall Manager

Last Modified: Friday, May 12, 2017

Event Source Product Information:

Vendor: [F5](#)

Event Source: Big-IP Advanced Firewall Manager

Version: 11.5

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later

Event Source Log Parser: bigipafm

Collection Method: Syslog

Event Source Class.Subclass: Security.Firewall

To configure the F5 Big-IP Advanced Firewall Manager event source, you must:

- I. Configure Syslog Output on F5 Big-IP Advanced Firewall Manager
- II. Configure NetWitness Suite for Syslog Collection

Configure Syslog Output on F5 Big-IP Advanced Firewall Manager

Note: These instructions are taken from the *BIG-IP® Network Firewall: Policies and Implementations* (Version 11.6) guide.

In the following procedures, we discuss only the required parameter changes needed to get the Big-IP AFM event source to communicate with RSA NetWitness Suite. For all other parameters, please see the *BIG-IP® Network Firewall: Policies and Implementations* (Version 11.6) guide for more details.

To configure the Big-IP AFM event source, perform the following tasks:

- I. Create a pool of remote logging servers
- II. Create a remote high-speed log destination
- III. Create a publisher
- IV. Create a custom Network Firewall Logging profile
- V. Configure an LTM virtual server for Network Firewall event logging

Create a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP system.

Create a pool of remote log servers to which the BIG-IP system can send log messages:

1. Open a browser window, and log onto the F5 Big-IP Configuration Utility.
2. On the Main tab, click **Local Traffic > Pools**.
The Pool List screen opens.
3. Click **Create**.
The New Pool screen opens.
4. In the **Name** field, type a unique name for the pool.
5. Using the **New Members** setting, add the IP address of your RSA NetWitness Suite

Log Decoder or RSA NetWitness Suite Remote Log Collector.

- a. Type an IP address in the Address field, or select a node address from the Node List.
- b. Type a service number in the **Service Port** field, or select a service name from the list.

Note: Typical remote logging servers require port 514.

- c. Click **Add**.
6. Click **Finished**.

Create a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP system.

Create a log destination of the Remote High-Speed Log type to specify that log messages are sent to a pool of remote log servers:

1. On the Main tab, click **System > Logs > Configuration > Log Destinations**.

The Log Destinations screen opens.

2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

The BIG-IP system is configured to send an unformatted string of text to the log servers.

5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select protocol **UDP**.
7. Click **Finished**.

Create a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources:

1. On the Main tab, click **System > Logs > Configuration > Log Publishers**.
The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click << to move the destination to the **Selected list**.
5. Click **Finished**.

Create a custom Network Firewall Logging profile

Create a custom Logging profile to log messages about BIG-IP system Network Firewall events:

1. On the Main tab, click **Security > Event Logs > Logging Profiles**.
The Logging Profiles list screen opens.
2. Click **Create**.
The New Logging Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.
5. In the Network Firewall area, from the **Publisher** list, select the publisher the BIG-IP system uses to log Network Firewall events.
6. Set an **Aggregate Rate Limit** to define a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged.
7. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules. You can select any or all of the options. When an option is selected, you can configure a rate limit for log messages of that type.

Option	Description
	Enables or disables logging of packets that match ACL rules configured with:

Option	Description
Accept	action=Accept
Drop	action=Drop
Reject	action=reject

8. Select the **Log IP Errors** check box, to enable logging of IP error packets. When enabled, you can configure a rate limit for log messages of this type.
9. Select the **Log TCP Errors** check box, to enable logging of TCP error packets. When enabled, you can configure a rate limit for log messages of this type.
10. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions. When enabled, you can configure a rate limit for log messages of this type.
11. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for Network Firewall log events.
12. Enable the **Log Geolocation IP Address** setting to specify that when a geolocation event causes a network firewall action, the associated IP address is logged.
13. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: <pre>"management_ip_address", "bigip_hostname", "context_type", "context_name", "src_ip", "dest_ip", "src_port", "dest_port", "vlan", "protocol", "route_domain", "acl_rule_name", "action", "drop_reason"</pre>
Field-List	This option allows you to: <ul style="list-style-type: none"> • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character.
User-Defined	This option allows you to: <ul style="list-style-type: none"> • Select from a list, the fields to be included in the log.

Option	Description
	<ul style="list-style-type: none">• Cut and paste, in a string of text, the order the fields display in the log.

14. Click **Finished**.

Assign this custom network firewall Logging profile to a virtual server.

Configure an LTM virtual server for Network Firewall event logging

Ensure that at least one log publisher exists on the BIG-IP system.

Assign a custom Network Firewall Logging profile to a virtual server when you want the BIG-IP system to log Network Firewall events on the traffic that the virtual server processes:

Note: These steps apply only to LTM[®]-provisioned systems.

1. On the Main tab, click **Local Traffic > Virtual Servers**.

The Virtual Server List screen opens.

2. Click the name of the virtual server you want to modify..

3. On the menu bar, click **Security > Policies**.

The screen displays firewall rule settings.

4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.

Note: If you do not have a custom profile configured, select the predefined logging profile global-network to log Advanced Firewall Manager™ events. Note that to log global, self IP, and route domain contexts, you must enable a Publisher in the global-network profile.



5. Click **Update** to save the changes.

Configure NetWitness Suite for 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.

Copyright © 2017 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners.