Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Barracuda Firewall NG F-Series Syslog

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Contents

Document Revision History

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to ArcSight Product Documentation Community on the Micro Focus Security Community.

Document Changes

Date	Product Version	Description
MM/DD/YYYY	X.X.X.X	Description of change

Configuration Guide for Barracuda Firewall NG F-Series Syslog SmartConnector

This guide provides information for installing the SmartConnector for Barracuda Firewall NG F-Series Syslog and configuring the device for syslog event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectors to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the documentation site for ArcSight SmartConnectors.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

The Barracuda NextGen (NG) Firewall F-Series is a family of hardware, virtual, and cloud-based appliances that protect and enhance your dispersed network infrastructure. They deliver advanced security by tightly integrating a comprehensive set of next-generation firewall technologies, including Layer 7 application profiling, intrusion prevention, web filtering, malware and advanced threat protection, antispam protection, and network access control.

The product uses syslog messages as a means of logging. The messages are sent to a text file on the Security Gateway, as well as to a remote server configured by the product administrator.

Configuration

For complete information about monitoring and logging Barracuda Firewall NG F-Series devices, see https://campus.barracuda.com/product/nextgenfirewallf/article/NGF71/Logs/. The information in this section is derived from that documentation.

Configuring Logging

Configuring logging requires the following steps:

- Configure Log Daemon
- Enable Audit Logs
- Configure Syslog Streaming
- Configure Web Log Streaming

Configuring Log Daemon

To configure the log daemon:

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Log Configuration**.
2. Click **Lock**.
3. Set the parameters for **Generate Log Data** and **Store Log Data**. For logs to be sent to the syslog service and written to disk, select **Yes** for both **Generate Log Data** and **Store Log Data**.
4. Click **Send Changes and Activate**.

Enabling Audit Logs

To activate the generation of Firewall audit data:

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > General Firewall Configuration**.
2. In the left menu, select **Audit and Reporting**.
3. From **Configuration Mode**, select **Switch to Advanced View**.
4. Click **Lock**.
5. In the **Log Policy** section, enable **Generate Audit Log**.
6. Click **Set** next to **Audit Log Data**.
7. From the **Audit Delivery** list, select **Syslog-Proxy**.

8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Configuring Syslog Streaming

The syslog streaming configuration defines the handling of log files. Log messages of centrally managed firewalls can be transmitted to the NextGen Control Center Syslog service, but they can also be transmitted to any other system designed for log file collection or to another Barracuda NextGen Firewall F-Series.

To configuring syslog streaming, complete the following steps:

- Enable the Syslog Service
- (Optional) Upload External SSL Certificates
- Configure Logdata Filters
- Configure Log Stream Destinations

Enabling the Syslog Service

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. Under **Operational Setup**, set **Enable Syslog Streaming** to **yes**.
4. Click **Send Changes** and **Activate**.

Uploading External SSL Certificates

If the syslog stream is SSL encrypted, by default the box certificate and key are used. To upload custom SSL certificates:

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.
3. In the left menu expand the **Configuration Mode** section and click **Switch to Advanced View**.
4. From the **Use Box Certificate/Key** drop-down list select **no**.
5. Import the **SSL Private Key** and **SSL Certificate**.
6. Click **Send Changes** and **Activate**.

Configuring Logdata Filters

Define profiles specifying the log file types to be streamed.

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.

2. In the left menu, select **Logdata Filters**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. Click the plus (+) icon to add a new entry.
6. Enter a descriptive name in the **Filters** dialog and click **OK**.
7. In the **Data Selection** table, you can add the log files to be streamed. Select **Firewall_ Audit_Log**.
8. In the **Affected Box Logdata** section, define what kind of box logs are to be affected by the syslog daemon from the **Data Selection** list.
9. When choosing **Selection** (default):
   a. Click the plus (+) icon next to **Data Selection** to add an entry
   b. Enter a descriptive name for the group and click **OK**. The **Data Selection** window opens
   c. Add the **Log Groups** for selection or select **Other** and specify an explicit selection.
   d. Set a **Log Message Filter**. When choosing **Selection**, add the explicit log type to the **Selected Message Types** table.
   e. Click **OK**.
10. Click **Send Changes** and **Activate**.

Configuring Logstream Destinations

You must configure a logstream destinationor selective syslog streaming.

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Syslog Streaming**.
2. In the left menu, select **Logstream Destinations**.
3. Expand the **Configuration Mode** menu and select **Switch to Advanced View**.
4. Click **Lock**.
5. Click the plus (+) icon to add a new entry.
6. Enter a descriptive name in the upcoming dialog and click **OK**.
7. Select the **Logtream Destination**. When an external log host is used, select **Explicit IP** (default) and enter the destination IP address in the Destination IP Address field.
8. Enter the **Destination Port** to deliver syslog messages.

   The Barracuda Networks CC syslog service listens on port TCP 5143 for SSL connections and on TCP and UDP port 5144 for unencrypted streaming. The default is to use encryption for delivery, therefore port 5143 is preconfigured. When changing the port, you must also adapt the host firewall rule for syslog traffic to use the new port.

9. Select either TCP or UDP as the **Transmission Mode**. UDP is the default option. However, for SSL connections TCP is automatically set.
10. Click **OK**.
11. Click **Send Changes** and **Activate**.

Configuring Web Log Streaming

Web Log streaming lets you send a syslog stream to an external device. Although TCP and TCP/TLS are supported as streaming protocols, UDP is recommended for performance reasons.

To stream an HTTPS session, the web traffic must match an access rule using SSL Interception. For HTTP traffic streaming no additional access rules are required.

Depending on the target device, it is possible to customize the log format to match the target device using streaming templates. For more information, see the Barracuda documentation.

Pre-requisites

When using the Barracuda Web Security Gateway as the destination syslog server, update the Web Security Gateway to the latest available firmware and contact Barracuda Networks Technical Support to set up your Web Security Gateway appliance.

Collect the following information for your destination device:

- Destination IP address
- Destination port
- Supported streaming protocols
- Log format
- Syslog facility
- Syslog level

Configuring Web Log streaming comprises the following steps:

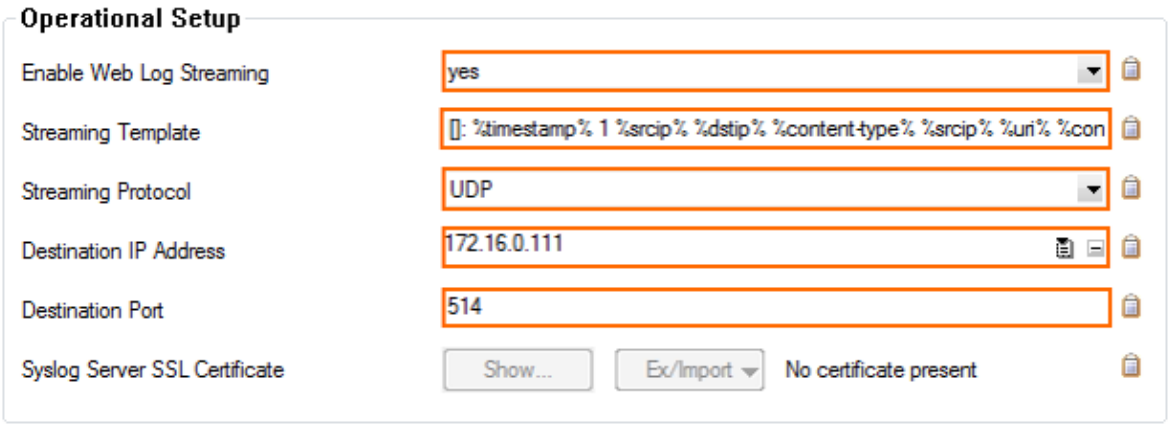
- Configure Web Log Streaming on the Firewall
- Create an Access Rule Matching HTTPS Traffic
- Configure the Syslog Service on the Destination Device

Configuring Web Log Streaming on the Firewall

Configure the Barracuda NG Firewall F-Series to stream every HTTP and HTTPS request to the configured syslog server using the streaming template as the log format.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. Click **Lock**.

3. In the left menu, click **Web Log Streaming**.
4. From the **Enable Web Log Streaming** drop-down list, select **yes**.



5. Enter the **Streaming Template** as required by the destination device. Use the **template placeholders** and plain text. The default value matches the required log format for the Barracuda Web Security Gateway.
6. Select the **Streaming Protocol**. Use **UDP** because it has the least performance impact on the F-Series.
7. Enter the **Destination IP Address**.
8. Enter the **Destination Port** (514 for the Barracuda Web Security Gateway).
9. Click **Send Changes** and **Activate**.

Creating an Access Rule Matching HTTPS Traffic (HTTPS Only)

To be able to stream information about HTTPS connections, ensure that the access rule matching the HTTPS traffic is using SSL Interception.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
2. Double-click to edit the access rule matching HTTPS traffic.
3. Click the **Application Policy** link and select **Application Control** and **SSL Interception**.
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Configuring the Syslog Service on the Destination Device

Configure the remote device running the syslog service to receive and process the syslog stream from the firewall.

Configuring for the Syslog SmartConnectors

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: `local1.warning @@10.0.0.1:514`

- To read all Syslog events, use *.*
- To filter specific events, replace regex with the specific event name.
- For example: *.* @@(remote/local-host-IP):514 and local1.warning @@10.0.0.1:514.
- To send events over a TCP connection, use @@ and to send events over an UDP connection, use @.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from

it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, syslogd is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as messages.log rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the /etc/rsyslog.conf file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

   ```
   mkfifo /var/tmp/syspipe
   ```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

   ```
   *.debug  /var/tmp/syspipe
   ```

   or

   ```
   *.debug  |/var/tmp/syspipe
   ```

3. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

   ```
   /etc/init.d/syslogd stop
   /etc/init.d/syslogd start
   ```

   or

   Execute the following command to send a configuration restart signal:

   On RedHat Linux:

   ```
   service syslog restart
   ```

   On Solaris:

```
kill -HUP `cat /var/run/syslog.pid´
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

   The syslog daemon is forced to reload the configuration and start writing to the pipe.
3. Restart the syslog daemon in one of the following methods:
   a. Restart the syslog daemon in one of the following methods:
   Enter the following commands:

   ```
   /etc/init.d/syslogd stop
   /etc/init.d/syslogd start
   ```

   or

   Execute the following command to send a configuration restart signal:

   On RedHat Linux:

   ```
   service syslog restart
   ```

   On Solaris:

   ```
   kill -HUP `cat /var/run/syslog.pid´
   ```

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the Micro Focus ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
  a. Click **Next**, the specify the following paramenters:

Parameters	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.

  b. **Click Next.**
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, the specify the following paramenters:

Parameters	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: `/var/tmp/syspipe`.
File Absolute Path Name	Specify the full path name for the file from which this connector will read events. The following are default values: • **Solaris:** `\var\adm\messages` • **Linux:** `\var\log\messages` You can use a wildcard pattern in the file name. In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation: • **Date format log rotation:** The device creates a new log at a specified time in the with the naming convention `filename.timestamp.log`. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new `filename.timestamp.log` and begins processing that file. To enable this log rotation, specify timestap in `yyyy-MM-dd` date format. For example, `filename.yyyy-MM-dd.log` • **Index log rotation:** The device writes to indexed files in the following format: `filename.log.001, filename.log.002, filename.log.003`, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:`filename'%d,1,99,true'.log;` Specifying `true` indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of `true` is optional.
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify **None**, **Rename**, or **Delete** as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value **None**.
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as **Rename**. The default value is **Processed**, which adds a `.processed` extension.

b. Click **Next.**

5. Select a destination and configure parameters.
6. Specify a name for the connector.

7. If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.
10. Run the SmartConnector.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Barracuda Firewall NG F-Series Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Panic = Very High; Security, Fatal, Error = High; Warning = Medium; Notice, Info, Internal = Low
Device Product	'Firewall NG F-Series'
Device Severity	Severity
Device Vendor	'Barracuda'
Old File Name	Log

Barracuda Firewall NG F-Series Web Streaming Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	emerg, crit, alerth = Very High; err = High; warning = Medium; info, notice, debug = Low
Destination Address	DestinationIP
Destination Host Name	Host
Device Action	ActionNum (0=ALLOWED, 1=BLOCKED)
Device Custom Number 1	ContentLength
Device Custom String 4	URLCategory
Device Event Class ID	'ALLOWED CLEAN'
Device Product	'Firewall NG F-Series'

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	Timestamp
Device Severity	_SYSLOG_PRIORITY
Device Vendor	'Barracuda'
File Type	ContentType
Name	'ALLOWED CLEAN'
Request URL	URI
Source Address	SourceIP
Source User Name	User

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on SmartConnector for Barracuda Firewall NG F-Series Syslog (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!