Netsurion™ | EventTracker

How to – Configure Barracuda NG Firewall to forward logs to EventTracker

EventTracker v8.x and above

Publication Date: May 20, 2019

Abstract

This guide provides instructions to configure **Barracuda NG Firewall F-Series** to send the syslog to EventTracker Enterprise. Once syslog is being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Essential** and **Barracuda NG Firewall F-Series** (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000).

Audience

Administrators who are responsible for monitoring **Barracuda NG Firewall F-Series** which are running using EventTracker Manager.

Table of Contents

Barracuda NG Firewall F-Series

The Barracuda NextGen 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.

In addition, the F-Series combines highly resilient VPN technology with intelligent traffic management and WAN optimization capabilities. This lets you reduce line costs, increase overall network availability, improve site-to-site connectivity, and ensure uninterrupted access to applications hosted in the cloud. Scalable centralized management helps you reduce administrative overhead while defining and enforcing granular policies across your entire dispersed network.

Prerequisites

- EventTracker v8.x and later should be installed.
- **Barracuda NG Firewall F-Series** (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000) should be installed and configured.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Configure Barracuda NextGen Firewall to send syslog to EventTracker

Logging into the Barracuda NextGen Firewall F-Series

1. Launch NextGen Admin.
2. Enter the Management IP, Username, and Password.

Figure 1

3. Click **Sign In**.

Configuring the Logstream Destinations

1. Configure the data transfer settings for the Eventtracker server. You can optionally choose to send all syslog data via an SSL-encrypted connection.
2. Go to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming.
3. In the left menu, select Logstream Destinations.
4. Click Lock.
5. Click + in the Destinations table. The Destinations window opens.
6. Configure the EventTracker server logstream destination
7. Enter the name “e.g. EventTracker”.
8. Remote Loghost – Select explicit-IP
9. Loghost IP Address – Enter the IP address of the EventTracker server.
10. Loghost Port – EventTracker server port.

Configuring Logdata Filters

Define profiles specifying the log file types to be transferred / streamed.

1. Go to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming.
2. In the left menu, select Logdata Filters.
3. Click Lock.
4. Click the + icon to add a new filter.
5. Enter a Name “e.g. FILT01” and click OK. The Filters window opens.
6. Click + in the Data Selection table and select Firewall_Audit_Log.
7. In the Affected Box Logdata section select Selection from the Data Selector dropdown.
8. Click + to add a Data Selection. The Data Selection window opens.
9. Enter a Name and click OK.
10. In the Log Groups table, click + and select Firewall-Activity-Only from the list.

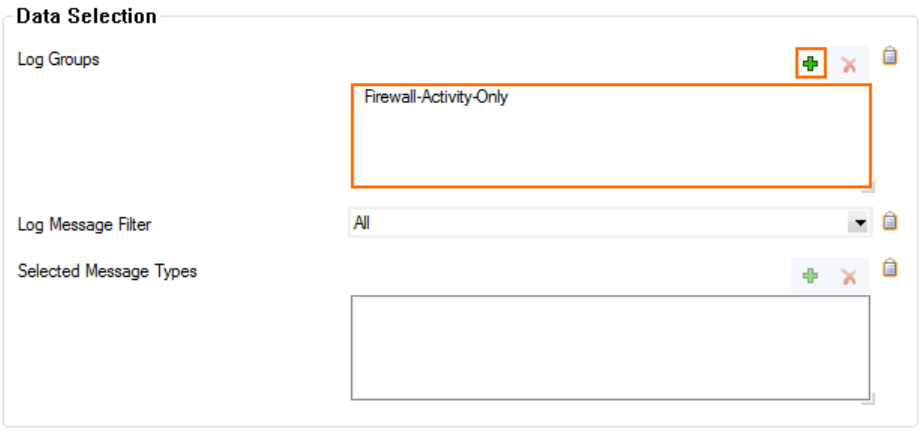

Figure 2

11. In the Data Selection Table, from the log message filter select the following filters.
    - Auth

- Config
- Firewall
- Network
- virscan
- wifi
- Watchdog

12. Click **OK**.
13. In the **Affected Service Logdata** section, select **None** from the **Data Selector** dropdown.
14. Click **OK**.

Enabling the Syslog Service

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

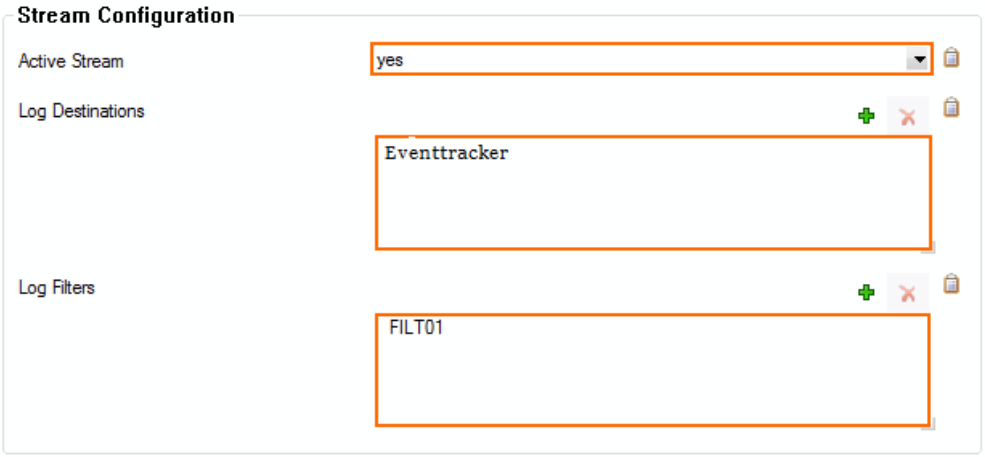

Figure 3

2. Set Enable the Syslog service to yes.
3. Click on + on log destination and select the Log Destination which we configured in the section Configuring the Logstream Destinations
4. Click on + on log filter and select the filter which we configured in the section Configuring Logdata Filters
5. Click Send Changes and Activate.