

# How to- Configure Barracuda Web Application Firewall to forward logs to EventTracker

EventTracker v9.0 and Above

Publication Date: June 14, 2019

### Abstract

This guide provides instructions to configure the Barracuda Web Application Firewall to send the syslog events to EventTracker.

#### Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Barracuda Web Application Firewall.

#### Audience

Barracuda Web Application Firewall Admins, who wish to forward syslog events to EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



## **Table of Contents**

Abstract	1
Scope	1
Audience	1
Overview	3
Prerequisites	3
Configuring Barracuda Firewall syslog	3
Adding Export Log Server	3
Adding Export Log Settings	5
Logs Format	8
Prerequisites Configuring Barracuda Firewall syslog Adding Export Log Server Adding Export Log Settings Logs Format	··· 3 ·· 3 ·· 5

# Netsurion... EventTracker

### Overview

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud.

Barracuda Web Application Firewall can be integrated with EventTracker using syslog. With the help of Barracuda Web Application Firewall KP items, we can monitor the network firewall logs, access logs, web firewall logs, system logs and audit logs on web applications. It also triggers the alert for authentication hijacking, buffer overflow attack, command injection attack, denial of service attack, and obfuscation attack.

## Prerequisites

- EventTracker v9.x or above should be installed.
- **Barracuda Web Application Firewall** should be installed and proper access permissions to make configuration changes.

# **Configuring Barracuda Firewall syslog**

### Adding Export Log Server

- 1. Go to the **ADVANCED > Export Logs** page.
- 2. In the **Export Logs** section, click **Add Export Log Server**. The **Add Export Log Server** window appears, specify values for the following:

#### Configure Barracuda WAF to forward logs to EventTracker

🖌 Barracuda	Web Applicatio	n Firewall					guest Sign out English
BASIC SECUR	ITY POLICIES WE	BSITES ACCESS	CONTROL AD	VANCED			Search help topics
ackups emplates ecure Administration	Energize Updates Vew Internal Patterns Troubleshooting	Firmware Update Libraries Vulnerability Reports	Export Logs Admin Access Co Cloud Control	Advanced Netwo ntrol High Availability Task Manager	rking Net App	work Firewall Logs searance	System Logs System Configuration
Export Logs		_	_	_		Add Export Log Se	Save Cance
Name Syslog	Server 10.5.21.25:514	Protoco Syslog	NG(udp)	Validate Server Certi. No	Comment	Actions Edit   Delet	•
Module Log Levels	MODULE	LOG	BLEVEL COMM	AENT			He
ogs Format	AAA	▼  0-E	mergency -		Add	J	14
Surlas Handar							
Systog Header.	Custon	n Header 👻					
web Filewall Logs For	mac	-					
Access Logs Format		•					
Audit Logs Format:		•					
Network Firewall Logs	Format Default	-	%t %un %lt %sl 9	6p %srci %srcp %di %	ip %act %acl	%dsc	
System Logs Format:	Default	•	%t %un %lt %md	%II %ei %ms			

Figure 1

- Name: Enter a name.
- Log Server Type: Select Syslog NG.
- IP Address: Enter the EventTracker IP address.
- **Port**: Enter the Syslog server (514) port.
- **Connection Type**: Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the EventTracker.
- Validate Server Certificate: Select No.
- Client Certificate: Select No.
- Log Timestamp: Select Yes.
- 3. Click Add.

# Netsurion... EventTracker

4

Web Application Firewall:	Add Export Log Server - Google Chrome -		×
🗎 waf.barracuda.com/	:gi-mod/index.cgi?password=8f0a3518fe54aabf5408cecdac13c937&et=1473	70686	48taut
Add Export Log Serve			Help
Name:			
Log Server Type:	Syslog NG -		
	Select the server type to which the logs needs to be exported.		
IP Address:	1.1.1.1		
D. d	The IP address of the log server.		
Port	514		
Connection Type:	The port associated with the IP address of the log server.		
oonnoonon type.	Select the connection type to transmit the loss from the Barracuda Web Annication Firewall to the		
	Sysbg server.		
Validate Server Certificate	⊖ Yes ⊛ No		
	Validates the syslog server certificate using the internal bundle of Certificate Authority's (CA's)		
Client Certificate:	Certificates packaged with the system. If set to No, any certificate from the systog server is accepted.		
	Set to Yes to validate the system server certificate using the internal bundle of Certificate Authority's		
	(CAs) certificates packaged with the system. If set to No, any certificate from the syslog server is		
Log Timestamp and	accepted.		
Hostname:	• Yes • No		
Comment	Logs the date and time of the system events,		
Add			
© 2016 Barracuda Networks, Inc.	Serial #BAR-WF-489542 Firmware v8.1.0.000 /2016-05-24	03:24:30	More
a parte denaceda (filmonda, inte	Figure 2		

### Adding Export Log Settings

- 1. Go to the **ADVANCED > Export Logs** page.
- 2. In the **Export Logs** section, click **Export Log Settings**. The **Export Log Settings** window appears, specify values for the following:



#### Configure Barracuda WAF to forward logs to EventTracker

	Web Applicatio	n Firewall						marti	
BASIC SECU		BSITES ACCESS C	ONTROL ADVAN	CED			Search help topics		
ckups nplates cure Administration	Energize Updates View Internal Patterns Troubleshooting	Firmware Update Libraries Vuinerability Reports	Export Logs Admin Access Contro Cloud Control	Advanced Networ High Availability Task Manager	king Network Appears	k Firewall Logs ance	System Logs System Configuration		
							Save	Can	
cport Logs					Ac	dd Export Log Se	erver Export Log Setti	ngs I	
Name	Server	Protocol		Validate Server Certi	Comment	Actions			
Syslog	10.5.21.25:514	Syslog N	G(udp)	No	Edit   Dele		de		
	AAA	• 0-Em	ergency -		Add				
ogs Format	AAA	▼ 0-Em	ergency -	•	Add				
ogs Format		- 0-Em	ergency -		Add			ŀ	
ogs Format Syslog Header:	AAA Custon	v 0-Em	ergency -		Add			1	
<b>ogs Format</b> Syslog Header: Web Firewall Logs Fo	AAA Custon	n Header	ergency V		Add			1	
<b>ogs Format</b> Syslog Header: Web Firewall Logs Fo Access Logs Format	Custon Custon iormat: : t	n Header	ergency V		Add			,	
ogs Format Syslog Header: Web Firewall Logs Fo Access Logs Format Audit Logs Format	Format:	n Header •	ergency V		Add			•	
ogs Format Syslog Header: Web Firewall Logs Fo Access Logs Format Audit Logs Format Network Firewall Log	Custon Custon Format: : t gs Format: Default	n Header •	ergency V	* %srci %srcp %di %dj	Add	lsc		,	
ogs Format Syslog Header: Web Firewall Logs Fo Access Logs Format Audit Logs Format Network Firewall Log System Logs Format	Format: Custon cormat: : t gs Format: Default t Default	• 0-Em	St %un %it %si %p %t %un %it %si %p	° %srci %srcp %di %d  %ei %ms	Add p %act %acl %d	lsc		•	
ogs Format Syslog Header: Web Firewall Logs Fo Access Logs Format Audit Logs Format Network Firewall Log System Logs Format	Custon format: : t	n Header	EVEL COMMEN ergency - %t %un %lt %sl %p %t %un %lt %md %l	* %srci %srcp %di %dj %ei %ms	Add p %act %acl %d	lsc		ł	

#### Figure 3

- 3 In the syslog settings section of the **Export Log Settings** dialog box, follow the below-mentioned screenshot process.
- 4 Click Save.

# Netsurion... EventTracker

Web Application Firewall: Ex	port Log Settings - Google Chrome	- 0		×
waf.barracuda.com/co	gi-mod/index.cgi?password=45d608342f28c78b40e54cae25bc9b6 <mark>3&amp;</mark> et=	1473	71010	98(a
	Save		Cancel	)
xport Log Settings				lelp
Export Web Firewall Logs	Enable     Disable			
Export Access Logs	<ul> <li>Enable</li> <li>Disable</li> </ul>			
Export Audit Logs	<ul> <li>Enable @ Disable</li> </ul>			
Export System Logs	Set to Enable to export audit logs to the configured log server.  Enable  Disable			
Export Network Firewall Logs	Set to Enable to export system logs to the configured log server.   Enable  Disable Set to Enable to export network frewail logs to the configured log server.			
xport Log Filters				lelp
Web Firewall Log Severity	6-Information -			
System Log Severity	6-Information			
yslog Settings	lecal0 =			lelp
	Select the log facility to export web firewall logs to the configured syslog server. Web Firewall Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts			
Access Logs Facility	loans the same systop server. Iocal0  Select the log facility to export access logs to the configured systop server. Access Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same systop server.			
Audit Logs Facility	local0 - Select the kg facility to export audit logs to the configured syslog server. Audit Logs Facility is used to identify the Barracuda Web Application Firewal and distinguish it from other hosts using the same syslog			
System Logs Facility	Iocal0  Select the log facility to export system logs to the configured syslog server. System Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same such a severe.			
Network Firewall Logs	local0 -			
Facility	Select the log facility to export network frewall logs to the configured syslog server. Network Firewall Log Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.			

Figure 4

Netsurion... EventTracker

#### Logs Format

Barracurta	Web Applicat	ion Firewa								guest Sign out Eng	pish 🔻
			ACCESSIC		0.50				Sea	ch help topics	٩
Backups Templates Secure Administration	Energize Updates Vew Internal Patterns Troubleshooting	Firmware Libraries Winerabil	Update ty Reports	Export Logs Admin Access Control	ol	Advanced Networ High Availability Task Manager	king	Network Firewall Lo Appearance	gs Syst Syst	em Logs em Configuration	
Export Logs								Add Export	Log Server	Export Log Sett	ings Help
Name	Server		Protocol		Valid	ate Server Certi	Comment	Acti	ons		_
Syslog	10.5.21.25:514		Syslog NO	3(udp)	No			Edit	Delete		
Module Log Levels	•										Help
NAME	MODULE		LOGI	EVEL COMME	ιτ						
	AAA 🔨		▼ 0-Em	ergency -			A	bd			
Logs Format											Help
System Header	0										
Systey Header.	Cust	tom Meader									
Web Firewall Logs For	:		•								
Access Logs Format			•								
Audit Logs Format			•								
Network Firewall Logs	Format Defa	ult	•	%t %un %lt %sl %p	%srci	%srcp %di %dj	p %act %	acl %dsc			
System Logs Format:	Defa	ult	•	%t %un %lt %md %	I %ei	%ms					
Custom Headers											Help

#### Figure 5

- 1. From the Web Firewall Logs Format list box, select Custom Format.
- In the Web Firewall Logs Format field, type the following custom event format: t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au
- 3. From the Access Logs Format list box, select Custom Format.
- 4. In the Access Logs Format field, type the following custom event format: t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu
- 5. From the Audit Logs Format list box, select Custom Format.
- In the Audit Logs Format field, type the following custom event format: t=%t|trt=%trt|an=%an|li=%li|lp=%lp18.
- 7. From the Network Firewall Logs Format list box, select Default.
- 8. From System Logs Format list box, select Default.
- 9. Click Save Changes.

Barracuda Web Application Firewall events are automatically discovered. Events forwarded to EventTracker by Barracuda Web Application Firewall are displayed on the Log Search tab of EventTracker.

