

Integrate Barracuda Web Application Firewall 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	
Scope	1
Audience	1
Overview	
Prerequisites	
Configuring Barracuda Firewall syslog	
Adding Export Log Server	
Adding Export Log Settings	5
Logs Format	
EventTracker Knowledge Pack (KP)	9
Categories	
Alerts	
Importing Barracuda Firewall Knowledge pack into EventTracker	
Category	
Alerts	
Verifying Barracuda Firewall knowledge pack in EventTracker	
Categories	
Alerts	15



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:

BASIC SECUR	BITY POLICIES	WEBSITES	ACCESS	CONTROL ADVA	NCED			Search help topics	
ckups mplates cure Administration	Energize Update: View Internal Patt Troubleshooting	erns Libra	ware Update tries erability Reports	Export Logs Admin Access Contro Cloud Control	Advanced Networ rol High Availability Task Manager	-	etwork Firewall Logs opearance	System Logs System Configuration	
								Save	
xport Logs							Add Export Log Se	erver Export Log Setting	gs He
Name	Server		Protoc	ol	Validate Server Certi	Comment	Actions		
Syslog	10.5.21.25	514	Syslog	NG(udp)	No		Edit Delet	te	
NAME	s MOD AAA	ЛЕ		G LEVEL COMMEN	NT	Add			н
NAME	MOD	ILE			NT	Add			He
NAME	MOD AAA	ULE Custom Heade	▼ 0-E	mergency -	NT	Add			
.ogs Format	MOD AAA		▼ 0-E	imergency -	NT	Add			
NAME .ogs Format Syslog Header:	MOD AAA		• 0-E	imergency -	NT	Add			
NAME ogs Format Syslog Header: Web Firewall Logs For	MOD AAA		• 0-E	imergency	NT	Add			
NAME .ogs Format Syslog Header: Web Firewall Logs For Access Logs Format:	MOD → AAA () () () () () () () () () ()		• 0-E	imergency					

- 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.

Web Application Firewall: A	Add Export Log Server - Google Chrome -		×
waf.barracuda.com/c	gi-mod/index.cgi?password=8f0a3518fe54aabf5408cecdac13c937&et=1473	70686	481a
Add Export Log Server			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		
	The IP address of the log server.		
Port	514		
	The port associated with the IP address of the log server.		
Connection Type:	UDP O TCP O SSL		
	Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the		
Validate Server Certificate:	Syslog server.		
	Validates the syslog server certificate using the internal bundle of Certificate Authority's (CA's) certificates packaged with the system. If set to No, any certificate from the syslog server is accepted.		
Client Certificate:	Ves No		
	Set to Yes to validate the syslog 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 accepted.		
Log Timestamp and	Yes O No		
Hostname:	Logs the date and time of the system events.		
Comment			
Add			
016 Barracuda Networks, Inc.	Serial #BAR-WF-489542 Firmware v8.1.0.009 (2016-05-24	03:24:30)) Mor
	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:



Integrate Barracuda Web Application Firewall

BASIC SECUR	RITY POLICIES WE	BSITES ACC	ESS CONTROL	ADVANCED				Sear	rch help topics	
ckups mplates cure Administration	Energize Updates View Internal Patterns Troubleshooting	Firmware Update Libraries Vulnerability Repo	Admin Acce	ess Control	Advanced Networ High Availability Task Manager	-	etwork Firewall Logs spearance		lem Logs lem Configuration	
									Save	_
xport Logs							Add Export Log	Server	Export Log Setting	s I
Name	Server	Pr	otocol	Vali	date Server Certi	Comment	Actions			
Syslog	10.5.21.25:514	Sys	slog NG(udp)	No			Edit De	lete		
Iodule Log Levels	s MODULE ≯ AAA	•		COMMENT		Add				1
NAME	MODULE	•		COMMENT		Add				,
.ogs Format	MODULE		0-Emergency -	COMMENT		Add				
NAME .ogs Format Syslog Header:	AAA Custon	• Header	•	COMMENT		Add				
NAME	AAA Custon		0-Emergency -	COMMENT		Add				
NAME .ogs Format Syslog Header:	AAA Custon		•	COMMENT		Add				
NAME cogs Format Syslog Header: Web Firewall Logs For	AAA Custon		•	COMMENT		Add				
NAME Cogs Format Syslog Header: Web Firewall Logs For Access Logs Format	MODULE AAA Custon rmat:	a Header	0-Emergency ▼		i %srcp %di %dj		1			

Figure 3

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

Web Application Firewall: E	ort Log Settings - Google Chrome	-		×
waf.barracuda.com/c	gi-mod/index.cgi?password=45d608342f28c78b40e54cae25bc9l	o63&et=14	7371010	986
		Save	Cancel)
Export Log Settings				Help
				0.2
Export Web Firewall Logs	Enable O Disable			
	Set to Enable to export web firewall logs to the configured log server.			
Export Access Logs	Enable Disable			
2/11/11/11/11/11/11/11/11/11/11/11/11/11	Set to Enable to export access logs to the configured log server.			
Export Audit Logs	Enable O Disable			
	Set to Enable to export audit logs to the configured log server.			
Export System Logs	Enable Disable			
Export Network Firewall	Set to Enable to export system logs to the configured log server.			
Logs	Enable Disable			
	Set to Enable to export network frewall logs to the configured log server.			
xport Log Filters				Help
Web Firewall Log Severity	6-Information -			
	Select the severity level to export web frewall logs to the configured log server.			
System Log Severity	6-Information -			
	Select the severity level to export system logs to the configured log server.			
Syslog Settings			1	Help
				0.00
Web Firewall Logs Facility	local0 -			
	Select the log facility to export web firewall logs to the configured syslog server. Web Firewal			
	Facility is used to identify the Barracuda Web Application Firewall and distinguish it from othe using the same syslog server.	r nosta		
Access Logs Facility	local0 -			
	Select the log facility to export access logs to the configured syslog server. Access Logs Fa	icility is		
	used to identify the Barracuda Web Application Firewall and distinguish it from other hosts usi			
	syslog server.			
Audit Logs Facility	local0 -			
	Select the log facility to export audit logs to the configured syslog server. Audit Logs Facility			
	identify the Barracuda Web Application Firewall and distinguish it from other hosts using the s server.	ame sysiog		
System Logs Facility	local0 -			
	Select the log facility to export system logs to the configured syslog server. System Logs Fa	cility is		
	used to identify the Barracuda Web Application Firewall and distinguish it from other hosts usi			
	syslog server.			
Network Firewall Logs Facility	local0 -			
racility	Select the log facility to export network frewall logs to the configured systeg server. Network			
	Log Facility is used to identify the Barracuda Web Application Firewall and distinguish it from using the same syslog server.	ouver nosts		
016 Barracuda Networks, Inc.	Secial #BAR-WF-489542 Firmware v8.1	0.009 (2016-05-	24.02.24.25	
o to danacous networks, Inc.	actual inclusion and a constrained of the second se	0.000 (5010-00-		TABILITY OF

Logs Format

Barracuda	Web Application	n Firewall					guest Sign out English	•
		BSITES ACCESS CO	NTROL ADVANC	ED		Sea	irch help topics	٩
Backups Templates Secure Administration	Energize Updates View Internal Patterns Troubleshooting	Firmware Update Libraries Waterability Reports	Export Logs Admin Access Control Cloud Control	Advanced Netwo High Availability Task Manager	rking Network I Appearan		tem Logs tem Configuration	
Export Logs					Add	d Export Log Server	Export Log Settings	Help
Name	Server	Protocol		Validate Server Certi	Comment	Actions		_
Syslog	10.5.21.25:514	Syslog NG	i(udp) N	0		Edit Delete		
Module Log Levels	MODULE AAA	Log L ▼ 0-Eme			Add			Help
Logs Format								Help
Syslog Header:	Custom	Header •						
Web Firewall Logs Form	nat.	•						
Access Logs Format		•						
Audit Logs Format		•						
Network Firewall Logs	Format Default	• 5	%t %un %lt %sl %p %	srci %srcp %di %d	lp %act %acl %ds	c		
System Logs Format:	Default	• •	%t %un %lt %md %ll 9	iei %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.
- 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.



EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Alerts and, categories can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v9.x to support Barracuda Web Application Firewall monitoring:

Categories

- **Barracuda: Application platform exploits** This category based report provides information related to application platform exploit.
- **Barracuda: Authentication hijacking** This category based report provides information related to authentication hijacking.
- **Barracuda: Buffer overflow attack** This category based report provides information related to buffer overflow attack.
- **Barracuda: Command injection attack** This category based report provides information related to the command injection attack.
- **Barracuda: Cookie poisoning attack** This category based report provides information related to a cookie poisoning attack.
- **Barracuda: Cross-site scripting attack** This category based report provides information related to cross-site scripting attack.
- **Barracuda: Denial-of-service attack** This category based report provides information related to the denial-of-service attack.
- **Barracuda: Directory traversal attack** This category based report provides information related to directory traversal attack.
- **Barracuda: Error message interception** This category based report provides information related to error message interception.
- **Barracuda: Firewall received messages** This category based report provides information related to firewall received messages.
- Barracuda: Firewall scan messages This category based report provides information related to firewall scan messages.



- **Barracuda: Firewall sending messages** This category based report provides information related to firewall sending messages.
- **Barracuda: Forceful browsing attack** This category based report provides information related to forceful browsing attack.
- **Barracuda: Form tampering attack** This category based report provides information related to form tampering attack.
- **Barracuda: Malicious file execution attack** This category based report provides information related to the malicious file execution attack.
- **Barracuda: Obfuscation attack** This category based report provides information related to obfuscation attack.
- **Barracuda: Protocol exploit attack** This category based report provides information related to protocol exploit attack.
- **Barracuda: SQL injection attack** This category based report provides information related to the SQL injection attack.
- Barracuda: Traffic allowed This category based report provides information related to traffic allowed.
- Barracuda: Traffic denied- This category based report provides information related to traffic denied.

Alerts

- Barracuda: Authentication hijacking- This alert is generated when authentication hijacking occurs.
- Barracuda: Buffer overflow attack- This alert is generated when a buffer overflow attack occurs.
- Barracuda: Command injection attack- This alert is generated when command injection attack occurs.
- Barracuda: Cookie poisoning attack- This alert is generated when a cookie poisoning attack occurs.
- Barracuda: Cross-site scripting attack- This alert is generated when cross-site scripting attack.
- Barracuda: Denial-of-service attack- This alert is generated when a denial-of-service attack occurs.
- Barracuda: Error message interception- This alert is generated when error message interception occurs.

- Barracuda: Malicious file execution attack- This alert is generated when a malicious file execution attack occurs.
- Barracuda: Obfuscation attack- This alert is generated when the obfuscation attack occurs.

Importing Barracuda Firewall Knowledge pack into EventTracker

- 1. Launch the EventTracker Control Panel.
- 2. Double click Export/Import Utility, and then click the Import tab.

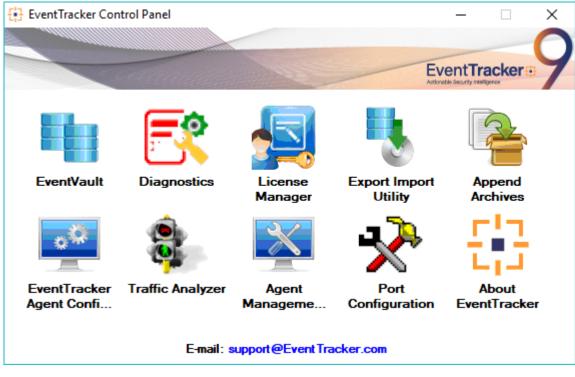


Figure 6

3. Import Category and Alerts as given below.

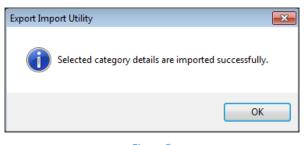
Category

1. Click **Category** option, and then click the browse **L** button



🐁 Export Import Utility	—		Х
Export Import			
 Provide the path and file name of the Categories file. Use the '' button to browse and locate the import file. Click the Import button. 			
Options			
Category			
⊖ Filters			
⊖ Alerts			
O Systems and Groups Source : *iscat			
O Token Value			
⊖ Reports			
O Behavior Correlation			
Ir	nport	Clos	se

- 2. Locate All Barracuda firewall group of Categories.iscat file, and then click the Open button.
- 3. Click the **Import** button to import the categories.
- 4. EventTracker displays a success message.





5. Click **OK**, and then click the **Close** button.

Alerts

1. Click the **Alert** option, and then click the browse **button**.

 Provide the path and file na Click the Import button. 	me of the Alerts file. Use the '' butt	on to browse and locate the import file.	
Options O Category	Location Import E-mail settings		
Galegoly Filters Alerts	Set Active Only if notifications set Dy default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.	
Systems and Groups Token Value Reports		or alerts which have Advanced watchlist configured. he user should make sure the watchlist groups are available	
Behavior Correlation	Source :		
	aduit		

Figure 9

- 2. Locate All Barracuda firewall group of Alerts.isalt file, and then click the Open button.
- 3. Click the **Import** button to import the alerts.
 - EventTracker displays a success message.



Figure 10

4. Click **OK**, and then click the **Close** button.



Verifying Barracuda Firewall knowledge pack in EventTracker

Categories

- 1. Login to EventTracker.
- 2. Click the Admin menu, and then click Category.

≡	Event Tracker @				🔎 🛛 Admin 🗸	Tools 🗸
	Home		Active Watch Lists	Event Filters	🧭 Parsing Rules	
q		_	Alerts	Sector Eventvault	Report Settings	
	0	0	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
			🗞 Behavior Correlation Settings	Group Management	🙊 Users	
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Cor USB activities, New		Q IP Lookup Configuration	r Weights	orting Syste ot reporting si
			● Category	· 🔆 Knowledge Objects	Windows Agent Config	
	Attacker		Diagnostics	Manager		

Figure 11

3. Click the search, and then search with Barracuda.

ategory			🔒 / Admin / Catego
Category Tree Search	Total category groups: 30 Total categories: 356 Last 10 modified categories		
barracuda 🔍 🔍	Name	Modified date	Modified by
Category	Barracuda: Application platform exploit	Jun 12 05:38:35 PM	
✓ Barracuda: Application platform	Barracuda: Authentication hijacking	Jun 12 05:38:35 PM	
exploit	Barracuda: Buffer overflow attack	Jun 12 05:38:35 PM	
→ Barracuda: Authentication hijacking	Barracuda: Command injection attack	Jun 12 05:38:35 PM	
✓ Barracuda: Buffer overflow attack	Barracuda: Cookie poisoning attack	Jun 12 05:38:35 PM	
vBarracuda: Command injection attack	Barracuda: Cross-site scripting attack	Jun 12 05:38:35 PM	
✓ Barracuda: Cookie poisoning attack	Barracuda: Denial-of-service attack	Jun 12 05:38:35 PM	
w Barracuda: Cross-site scripting attack	Barracuda: Directory traversal attack	Jun 12 05:38:35 PM	
Barracuda: Denial-of-service attack	Barracuda: Error message interception	Jun 12 05:38:35 PM	
✓ Barracuda: Directory traversal attack	Barracuda: Firewall received messages	Jun 12 05:38:35 PM	
✓Barracuda: Error message interception			
Barracuda: Firewall received			

Figure 12

Alerts

- 1. Login to EventTracker.
- 2. Click the Admin menu, and then click Alerts.

	Event Tracker ⊕					🔎 🛛 Admin-	Tools -
-	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashi
q		_	Alerts	C Correlation	Q IP Lookup Configuration	🛱 Users	
	0	2	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	1 Weights	
			🗞 Behavior Correlation Settings	😴 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			Gategory Category Category	FAQ Configuration	Report Settings		
	Attacker			 News 			



3. In the **Search** box, type **'Barracuda'**, and then click the **search**. Alert Management page will display all the imported alerts.

Show All	v							Search by	Alert name	 ★ / Admin / Alert > barracuda Q Q
153 Available Aler Total number of a		46 Active Alerts Total number of active alerts			Sy	53 /stem/User [punt for system a				Cricial 17 Low 16 19 Serious 14 23 by Threat Level alerts by threat level
⊕ Î	Activate Now Click 'Activat	e Now' after making all changes								Total: 9 Page Size 25 ~
	Alert Name ٨		Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
□ 🖓 Barrac	cuda: Authentication hijacking		•							
Barrac	cuda: Buffer overflow attack		•							
C 양성 Barrac	cuda: Command injection attack		•							
음 양 Barrac	cuda: Cookie Poisoning attack		•							
🗆 දීංචි Barrad	cuda: Cross-site scripting attack		•							
Barrac	cuda: Denial-of-service attack		•							
🗆 🖗 Barrad	cuda: Error message interception		•							
Barrac	cuda: Malicious file Execution at	ack	•							
🗆 🖗 Barrac	cuda: Obfuscation attack		•							

Figure 14

4. To activate the imported alerts, select the respective checkbox in the Active column.

EventTracker displays a message box.





5. Click **OK**, and then click the **Activate Now** button.

NOTE: Specify appropriate **systems** in the **alert configuration** for better performance.