# Netsurion. EventTracker\*

# Integrate Zyxel Firewall EventTracker v9.2 and later

Publication Date: January 13, 2021

## Abstract

This guide provides instructions to retrieve the **Zyxel firewall** events by syslog. After **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor the **Zyxel firewall**.

### Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Zyxel** firewall USG60(W), USG 310, USG110.

# Audience

Administrators who are assigned the task to monitor **Zyxel firewall** events using 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 Zyxel firewall 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.

© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



# Table of Contents

1.	Intr	oduction	. 3
2.	Prei	requisites	. 3
3.	Con	figuring Zyxel firewall Syslog logging	3
4.	Eve 4.1	ntTracker Knowledge Pack Categories	4 5
	4.2	Reports	5
	4.3	Dashboards	6
5.	Imp 5.1	orting knowledge pack into EventTracker Categories	8 9
	5.2	Flex Reports 1	10
	5.3	Knowledge Objects 1	12
	5.4	Dashboards 1	13
6.	Veri 6.1	ifying knowledge pack in EventTracker	L5 15
	6.2	Flex Reports 1	15
	6.3	Knowledge Objects 1	16
	6.4	Dashboards 1	17



# 1. Introduction

Zyxel firewalls are next-generation firewalls designed to deliver high availability, anti-malware protection, and consolidated policy enforcement for medium to large-sized businesses and campuses.

Zyxel firewall when configured sends events to EventTracker using syslog. Zyxel Firewall sends events like antivirus scan, intrusion detection and prevention, anti-spam, anti-virus, content filtering, unified security policy, IPsec VPN, SSL VPN, and WLAN management. Generates reports on antivirus spam detail, intrusion activities, configuration changes, interface statistics, traffic denied, etc. It contains username, client IP address, status, message, action, file path, file name, and hash. Graphically displays interface statistics, traffic denied by reason, traffic denied by IP address, threat detected by file name, device name, device IP, etc.

# 2. Prerequisites

- Administrative access on Zyxel firewall Console.
- EventTracker manager IP address.
- Allow port number 514 from the firewall end.

# 3. Configuring Zyxel firewall Syslog logging

- 1. Log into the Zyxel Web Interface.
- 2. Navigate to Configuration > Log & Report > Log Settings.

CONFIGURATION	Log Sett	ings			
11 Quick Setup	Log Sett	ings			
Wedess	20	at 💡 Arman	Q mathem		
E Network		Status	Norther	Log Format	Summary
Web Authentication     Hotspot     Hotspot     Security Policy     Cloud CNM     June	1	9	System Log	linternal	E-mail Server 1 Mail Server Mail Subject Send From Send Log to Send Alert to Sched Alert to
BWM     UTM Profile     Device HA     Gogect	2	9	System Log	linternal	E-mail Server 2 Mail Server, Mail Server, Send From Send Alert to Send Alert to School Alert to
E Los & Report	3	9	US8 Storage	Internal	US8 Status: none
Ernal Daily Report	4	9	Remote Server 1	VRP7/Syslog	Server Address Log Facility: Local 1
· Ing Second	5	9	Remote Server 2	VRPT/Syslog	Server Address. Log Facility: Local 1
	6	Ŷ	Remote Server 3	VRPT/Syslog	Server Address Log Facility: Local 1
	1	9	Remote Server 4	VRPT/Syslog	Server Address: Log Facility: Local 1

Figure 1

Netsurion. EventTracker

- 3. Choose a Remote Server.
- 4. Click Active.
- 5. Choose Log Format as VRPT/Syslog.
- 6. Enter the IP address of the EventTracker.
- 7. Select Local 7 in the Log Facility field.
- 8. Select the Categories you want to be logged (normal = default logs, debug = very detailed logs, disable

= no logs)

CONSTRUCTION	Log Se	dings						
TE Quest Sena	E Log Se	ttings						
D Licenting	12	TAY O Actions	C) tractante					
		No.	A COLONICE	Text Germal		S.main		
		0	Statem Lon	internal .		E-mail 9	lever 1	
				Edit log Calegory Setting - Remote Server 1		Mail Ge		2
				Log Settings for Remote Server				
	2		System Log	2 Active				
UTM Profile				Log Format:	VRPT/Syslog			
Colect				Server Address:	192 168 22 222	(Serv	er Name or IP Ad	(dress)
				Log Facility:	Local 7			
	3		USB Storage					
Email Duily Report	4	- <del>R</del>	Ramote Second 1	Active Log				
	5	Q.	Remote Server 2				Selection	
		9	Remote Server 3	Log Category ja		dsable	normal	debug
	7	0	Renote Server 4	ill Authenticate	-		0	0
				B TWM			0	0
	24	C Page 1	of 1   #   #   Show 50	B Device HA			0	0
				Lill File Manager			0	0
				III Hotspot			0	0
				License			.0	0
				III Log & Report		٠	•	0
				3 Network			0	0
				at Security				0
				B System			0	
				UTM .				
							DK	Cano

Figure 2

# 4. EventTracker Knowledge Pack

Once Zyxel firewall events are enabled and Zyxel firewall events are received in EventTracker, alerts and reports can be configured in EventTracker.

The following knowledge packs are available in EventTracker to support Zyxel firewall monitoring.



## 4.1 Categories

- **Zyxel Firewall: Traffic activities** This category provides events information related to traffic denied and allowed.
- **Zyxel Firewall: Interface activities** This category provides events information related to interface statistics like down, active, and inactive.

## 4.2 Reports

• **Zyxel Firewall – Interface activities** - This report provides information related to interface down, inactive, and active. It provides information like interface port address, packets sent, packets received, device ID, and port status.

#### Log\_Sample

Jan 06 12:27:29 Zyxel\_Firewall Computer:Zyxel\_Firewall, Dec 10 11:08:52 10.10.140.6 Dec 10 11:08:52 2020 FEDC-FWL02 src="0.0.0.0:0" dst="0.0.0.0:0"

msg="name=Port1,status=1000M/Full,TxPkts=737059398,RxPkts=1251804984,Colli.=0,TxB/s=94,RxB/s=0,UpTi me=29292:07:26" note="INTERFACE STATISTICS" user="unknown" devID="107befd06ce6" cat="INTERFACE STATISTICS"

#### Sample\_Report

LogTime	Computer	Device ID	Interface	Status	Packets Sent	<b>Received Packets</b>
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P4_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P5_EuroFibr	1000M/Full	33056619092	23795609027
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P4_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P3_Managmnt	1000M/Full	5	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	P2_Empty	Inactive	0	0
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	Port6	1000M/Full	537143631	907017725
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	Port4	Down	0	0

#### Figure 3

• **Zyxel firewall – Traffic denied –** This report provides information related to suspicious traffic denied. It provides information like username, source IP, source port, destination IP, destination port, direction, and reason.

Log\_Sample

Jan 06 12:27:22 Zyxel\_Firewall Computer:Zyxel\_Firewall, Dec 10 10:01:53 192.168.101.20 Dec 10 11:01:43 2020 EUDC-ZW310-43L47 src="192.168.8.5:50251" dst="192.168.100.66:8530" msg="Match default rule, DROP" note="ACCESS BLOCK" user="kenneth" devID="ec43f6fea270" cat="Security Policy Control" class="Access Control" ob="0" ob\_mac="00000000000" dir="ANY:ANY" protoID=6 proto="others"

Sample\_Report



LogTime	Computer	Device ID	Source IP Address	Source Port	Destination IP Address	Destination Port	Direction	Reason
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.1617.1	52128	192.16.100.50	8080	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.16.17.1	52124	192.16.100.50	8080	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.16.15.5	65387	192.16.100.200	23560	ANY:ANY	abnormal TCP flag attack detected, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.168.15.5	65387	192.168.100.200	23560	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	124.156.245.159	47603	192.168.10.186	5000	ANY:ANY	Match default rule, DNAT Packet, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	192.241.235.192	56845	194.247.63.253	50070	ANY:ANY	Match default rule, DROP
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	113.187.206.71	64988	89.20.164.162	445	ANY:ANY	Abnormal TCP flag attack detected, DROF
01/11/2021 04:15:55 PM	ZYXEL_FIREWALL-SYSLOG	ec43f6fea270	194.247.42.220	58927	194.247.63.253	445	ANY:ANY	Match default rule, DROP

Figure 4

# 4.3 Dashboards

#### • Zyxel Firewall - Interface status



Figure 5







• Zyxel Firewall - Traffic denied by reason



• Zyxel Firewall - Traffic denied by destination IP



Figure 7





• Zyxel Firewall - Traffic denied by Source IP

# 5. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.

# Netsurion. EventTracker



Figure 9

Export-Import Utility window opens.

💺 Export Import Utility	
Export Import	
<ol> <li>Provide the path and file nanoval 2. Click the Import button.</li> </ol>	me of the Categories file. Use the '' button to
Ontions	Location
optiona	
Category	
0.5	

Figure 10

3. Click the Import tab.

## 5.1 Categories

- 1. In Export-Import Utility window, select the Category option, and click Browse . ...
- 2. Navigate to the knowledge pack folder and select the file with the extension .iscat, like "Categories\_Zyxel firewall. iscat" and click Import.



🧏 Expo	rt Import Utility					_		$\times$
Export	Import							
1. Pro 2. Clie	ovide the path and file nam ck the Import button.	e of the Categor	ies file. Use the '' butt	on to browse and locate	e the import file.			
	ions Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	Location	Source : *iscat					
					Impo	rt	Close	e

Figure 11

EventTracker displays a success message.





### 5.2 Flex Reports

1. In Export-Import Utility window, select the Import tab. Click the Reports option, and choose New (\*.etcrx).



🐁 Export Import Utility		—		×
Export Import	o of Cohodulo Popost file. Lies the '-' butten to browne and locate the invest file.			
2. Click the Import button Note : If report(s) contains temp	late, first import template and proceed with exportimport utility.			
Options	Location			
◯ Category				
○ Filters				
◯ Alerts	Legacy (*.issch)     New (*.etcnx)			
Systems and Groups	Source : *issch			
O Token Value				
Reports				
Behavior Correlation				
	Import		Clos	æ

Figure 13

2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **.etcrx**, e.g. **Reports\_Zyxel firewall.etcrx.** 

🚼 Reports Import								
Note : If report(s) contains template, first import template a	and proceed with report import proces							
Select file *etcry								
Available reports	Available reports							
Title	Frequency Show all	•	Q Q					
	Sites Groups	Systems	Frequency	Runtime Type				
		-,						

Figure 14

3. Wait while reports populate. Select all the relevant reports and click Import

Netsurion. EventTracker°

Note: Set run time option is not applicat	ole for Defined Reports and Hourly Reports			
Set run time for report(s) from	AM ▼ at interval of minutes	Set ()		
Replace	to Replace	Assign systems		
		Note: Make sure that Site(s), $Group(s)$ and $System(s)$ selections are ve	alid.	$\otimes$



EventTracker displays a success message.



Figure 16

### 5.3 Knowledge Objects

1. Click Knowledge objects under the Admin option in the EventTracker web interface.

			🔎 Admin 🗸	Tools 🕶 \tag
П	Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Das
	Alerts	Sector Eventvault	Report Settings	
	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
	🗞 Behavior Correlation Settings	Group Management	QQ Users	
o <b>mi</b> or so	Casebook Configuration	Q IP Lookup Configuration	r Weights	Systems since the last 24 hours
	eten Category	·☆· Knowledge Objects	Windows Agent Config	
	▲ Diagnostics	Manager		



2. Click the **import object** icon.



Netsurion. EventTracker<sup>®</sup>



#### Figure 18

 A pop-up box appears, click "Browse" and navigate to the knowledge packs folder (type "C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) with the extension ".etko", e.g. "KO\_Zyxel firewall.etko" and click "Upload".

mport						
KO_ <product name="">.etko</product>	General Browse Upload					

#### Figure 19

4. Wait while EventTracker populates all the relevant knowledge objects. After the objects display, select the required ones, and click **Import**.



Figure 20

## 5.4 Dashboards

- 1. Login to the EventTracker web interface.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.
- 3. In My Dashboard, Click the Import button.



≡	Event <b>Tracker</b> ⊕			
	Home			
٩	My Dashboard			
	Threats			
	Incidents			
	Behavior Correlation			
	Change Audit			
	Compliance			



🔶 / Dashboard / My Dashboard			
+ 🖉 @ 🌣 İ 丁 🛛 🛈			
Import configuration			



- Click Browse and navigate to the knowledge pack folder (type C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs in the navigation bar) where .etwd, e.g. Dashboard\_Zyxel firewall.etwd is saved and click "Upload".
- 5. Wait while EventTracker populates all the available dashboards. Enable Select All and click Import.

Import				
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.				
🗖 Browse	Upload			
Available widgets				
✓ Select All				





Import Close



# 6. Verifying knowledge pack in EventTracker

### 6.1 Categories

- 1. Login to the EventTracker web interface.
- 2. Click Admin dropdown and click Categories.
- 3. In Category Tree to view imported categories, click the Search tab and enter Zyxel firewall in the search.

Category				
Category Tree Search				
Zyxel Q Q				
Category				
VZyxel Frewall: Interface activities				
VZyxel Frewall: Traffic denied				



# 6.2 Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.



Netsurion. EventTracker

R	Report Configuration
	Report Dashboard
	Explorer

Figure 26

- 2. In the Reports Configuration pane, select the Defined option.
- 3. Click on the **Zyxel firewall** group folder to view the imported reports.

Report Configuration				
○ Scheduled ○ Queued	Defined			
Report Groups		ŧ		
Zyxel Firewall	Ű	1	*	



# 6.3 Knowledge Objects

16

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand the **Zyxel firewall** group folder to view the imported Knowledge objects.

Knowledge Objects		
Zyxel	Q	Q
Groups 🕀 🧭 🗓		
Zyxel Firewall		
Zyxel Firewall 🧭 📋		

Figure 28

## 6.4 Dashboards

1. In the EventTracker web interface, Click **Home** and select "**My Dashboard**".



Figure 29

2. In the **Zyxel firewall** dashboard the following screen appears.

A	vailable dashlets			×
	Zyxel			Q
	Zyxel Firewall - Interface status	Zyxel Firewall - Traffic denied by	Zyxel Firewall - Traffic denied by	Zyxel Firewall - Traffic denied by
				Export Close

Figure 30



