



**Integration Guide** 

# Integrate Forcepoint NGFW with the Netsurion Open XDR platform

**Publication Date:** 

February 27, 2023

© Copyright Netsurion. All Rights Reserved.



# Abstract

This guide provides instructions to configure the Data Source Integrations in the Netsurion Open XDR platform to receive the logs from the Forcepoint NGFW. The Data Source Integrations contains alerts, reports, dashboards, categories, and knowledge object.

#### Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

# Scope

The configuration details in this guide are consistent with Netsurion Open XDR platform version 9.3 or later and Forcepoint NGFW version 6.8.8 and later.

## Audience

This guide is for the administrators responsible for configuring the Data Source Integration in the Netsurion Open XDR platform.

# **Product Terminology**

The following are the terms used throughout this guide:

- The term "Netsurion's Open XDR platform" or "the Netsurion Open XDR platform" or "the Open XDR platform" refers to EventTracker.
- The term "Data Source Integrations" refers to Knowledge Packs.



# Table of Contents

1	Ove	erview	4
2	Pre	requisite	4
3	The	e Netsurion Open XDR platform Data Source Integration (DSI)	4
	3.1	Category	4
	3.2	Alerts	4
	3.3	Reports	5
	3.4	Dashboard	5
4	Imp	porting Forcepoint NGFW Data Source Integration into the Netsurion Open XDR	ł
pl	atfor	m	6
	4.1	Category	7
4	4.2	Alerts	8
4	4.3	Token Template	9
	4.4	Reports 1	0
	4.5	Knowledge Objects (KO)1	2
	4.6	Dashboard 1	4
5	Ver	ifying Forcepoint NGFW Data Source Integration in the Netsurion Open XDR	
pl	atfor	m1	6
	5.1	Category 1	6
	5.2	Alerts	7
	5.3	Token Template	8
	5.4	Reports 1	8
	5.5	Knowledge Objects (KO)1	9
	5.6	Dashboard	0



### 1 Overview

Forcepoint NGFW supports multiple components which provide services to inspect traffic logs, block malicious attacks, prevents data thefts etc. and all such events can be observed or managed by management console.

Netsurion's Open XDR platform seamlessly combines SIEM, Log Management, File Integrity Monitoring, Machine Analytics, and User Behavior Monitoring. The dashboard, category, alerts, and reports in Netsurion's Open XDR platform benefit in tracking critical activities, security warning activities, and others.

# 2 Prerequisite

Configure Forcepoint NGFW to forward logs to Netsurion Managed open XDR.

Note

Refer to <u>How-To</u> guide to configure Forcepoint NGFW to forward logs to Managed open XDR console.

# 3 The Netsurion Open XDR platform Data Source Integration (DSI)

After Netsurion's Open XDR platform receives the logs, configure the Data Source Integration in the Netsurion Open XDR platform.

The following Data source integration are available in the Netsurion Open XDR platform.

#### 3.1 Category

**Forcepoint NGFW - Events overview:** This category will provide detailed analysis on all events observed on Forcepoint NGFW firewall.

#### 3.2 Alerts

**Forcepoint NGFW: Critical events detected:** This alert will trigger when a critical level of severity events has been detected by Forcepoint NGFW.



#### 3.3 Reports

Forcepoint NGFW - Events overview: This report will capture all events performed on Forcepoint NGFW.

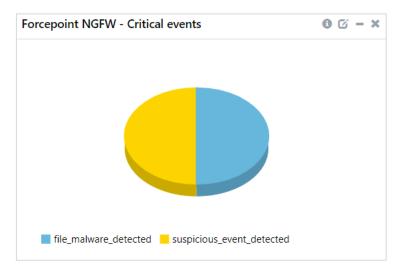
01/23/2023 02:54:00 AM Connection_Progress         0         MILCNT_sede node 2         192:168:10.36         5361         192:168:10.145         53         DNS (L           01/23/2023 02:54:00 AM Connection_Progress         0         Breacm node 2         192:168:10.36         5361         192:168:10.145         53         DNS (L           01/23/2023 02:54:00 AM Connection_Allowed         0         Breacm node 2         192:168:10.40         453         192:168:10.125         53         192:168:20.18         5842         192:168:20.125         53         DNS (L           01/23/2023 02:54:00 AM FW_New-Pase-VPN-Connection         0         Mercrn node 1         192:168:10.15         5876         192:168:10.14         5192         TCP/91           01/23/2023 02:54:00 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168:10.15         58876         192:168:10.14         5192         TCP/91           01/23/2023 02:54:00 AM Connection_Interface_Changed         0         MILCNT_sede node 1         53876         192:168:10.25         443         192:168:20.15         53761         192:168:20.15         543         HTTPS           01/23/2023 02:54:02 AM Connection_Interface_Changed         0         Breacm node 2         192:168:10.36         5361         192:168:10.21         53         TCP/91         TCP/91<	Pro		on NAT_Destination	T_Destination	NAT_Source 1		Destination								
3)1/23/2023 02:54:00 AM FW_Packet.Discarded       0       Brescnt node 2       192 168 10.40       \$453       192 168 10.21       \$3         1/123/2023 02:54:00 AM Connection_Allowed       0       Mercnt node 2       192 168 10.18       \$2097       Allow       192 168 10.125       \$3       192 168 20.18       \$8424       192 168 20.125       \$3       DNS (U         1/123/2023 02:54:00 AM Connection_Allowed       0       Mercnt node 1       192 168 10.16       \$5703       Allow       192 168 10.125       \$3       192 168 20.18       \$8424       192 168 20.125       \$3       DNS (U         1/123/2023 02:54:00 AM Connection_Interface_Changed       0       MILCNT_sede node 1       192 168 10.16       \$8878       192 168 10.62       \$43       192 168 20.15       \$3781       192 168 20.52       \$443       HTTPS         1/123/2023 02:54:00 AM Sample_Chical_Event       10       MILCNT_sede node 1       192 168 10.61       \$8878       192 168 10.52       \$43       192 168 20.51       \$3781       192 168 20.52       \$443       HTTPS         1/1/23/2023 02:54:02 AM Connection_Progress       0       MILCNT_sede node 1       192 168 10.61       \$53       192 168 10.21       \$53       192 168 20.15       \$192 168 20.15       \$192 168 20.15       \$192 168 20.12       \$192 168 20.12       \$102 108 20.12<	Type _ID	Protocol_Typ	_Port		P_Port	NAT_Source_IF	_Port	Destination_Address	Port Action	Source	Sender_Address	Component_ID	Severity	Event_Type	ogTime
1/1/23/2023 02.54.00 AM Connection_Allowed       5       Mercnt node 2       192.168.10.18       52097       Allow       192.168.10.125       5.3       192.168.20.18       58424       192.168.20.125       5.3       DNS (t         1/1/23/2023 02.54.00 AM Connection_Interface_Changed       5       Mercnt node 1       192.168.10.18       52097       Allow       192.168.10.14       5192       TCPP9         1/1/23/2023 02.54.00 AM Connection_Interface_Changed       5       MILCNT_sede node 1       192.168.10.15       58878       192.168.10.89       5443       192.168.20.15       53761       192.168.20.89       443       HTTPS         1/1/23/2023 02.54.00 AM Connection_Interface_Changed       5       MILCNT_sede node 1       192.168.10.85       53878       192.168.20.15       53781       192.168.20.15       5443       HTTPS         1/1/23/2023 02.54.02 AM Connection_Progress       5       MILCNT_sede node 1       192.168.10.18       53861       192.168.10.15       53       192.168.20.15       53       192.168.20.125       53       DNS (t         1/1/23/2023 02.54.02 AM FW_New-H9ec-VHCO       5       MILCNT_sede node 1       192.168.10.18       53861       192.168.10.15       53       192.168.20.15       53       DNS (t         1/1/23/2023 02.54.02 AM Connection_Progress       5       MI	P) 17	DNS (UDP)					53	192.168.10.145		63861	192.168.10.36	MILCNT_sede node 2	0	Connection_Progress	/23/2023 02:54:00 AM
31/23/2023 02:54:00 AM FW_New-Pasc-VPN-Connection_Interface_Changed         Mercnt node 1         192:168:10.68         53703         Allow         192:168:10.14         5192         TCPP           17/23/2023 02:54:00 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168:10.51         58878         192:168:10.52         443         192:168:20.51         53761         192:168:20.89         443         HTTPS           01/23/2023 02:54:00 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168:10.51         58878         192:168:10.52         443         192:168:20.15         53761         192:168:20.52         443         HTTPS           01/23/2023 02:54:02 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168:10.36         53861         192:168:10.145         53         192:168:20.15         53781         192:168:20.15         5402         MILCNT_sede node 2         192:168:10.36         53861         192:168:10.14         5102         53         192:168:20.18         5402         MICNT_sede node 2         192:168:10.36         53703         Allow         192:168:10.21         53         192:168:20.18         5402         MILCNT_sede node 1         192:168:10.36         53703         Allow         192:168:10.21         53         192:168:20.18         5402	17						53	192.168.10.21		4453	192.168.10.40	Brescnt node 2	ъ	FW_Packet-Discarded	/23/2023 02:54:00 AM
D1/23/2023 02:54:00 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168 10:5         58878         192:168:10.89         443         192:168:20.15         53781         192:168:20.89         443         HTTPS           D1/23/2023 02:54:00 AM Sample_Critical_Event         10         MILCNT_sede node 1         192:168:10.51         58878         192:168:10.52         443         192:168:20.51         53781         192:168:20.52         443         HTTPS           D1/23/2023 02:54:02 AM Connection_Progress         0         MILCNT_sede node 2         192:168:10.36         53861         192:168:10.145         53         DNS (L         DNS (L           D1/23/2023 02:54:02 AM FW_Packet-Discarded         0         Bescnt node 2         192:168:10.104         4453         192:168:10.125         53         192:168:20.18         5442         192:168:20.125         53         DNS (L           D1/23/2023 02:54:02 AM FW_Packet-Discarded         0         Mercent node 2         192:168:10.18         52097         Allow         192:168:10.15         53         192:168:20.18         5442         192:168:20.125         53         DNS (L           D1/23/2023 02:54:03 AM FW_New-Packet-Discarded         0         Mercent node 1         192:168:10.18         53/31         192:168:20.18         54/43         192:168:20.1	P) 17	DNS (UDP)	53	2.168.20.125	38424 1	192.168.20.18	53	192.168.10.125	Allow	52097	192.168.10.18	Mercnt node 2	ъ	Connection_Allowed	/23/2023 02:54:00 AM
3/12/32/022 30 2:54:00 AM Sample_Ortical_Event       10       MILCNT_sede node 1       192:168 10.51       58878       192:168:10.52       443       192:168:20.51       53781       192:168:20.52       443       HTTPS         3/12/32/022 30 2:54:02 AM Connection_Progress       0       MILCNT_sede node 2       192:168:10.61       53861       192:168:10.145       53       DNS (t         3/12/32/022 30 2:54:02 AM Connection_Progress       0       Bresont node 2       192:168:10.40       443       192:168:10.15       53       DNS (t         3/12/32/023 02:54:02 AM Connection_Allowed       0       Merch node 2       192:168:10.81       53       DNS (t       53       DNS (t         3/12/32/023 02:54:02 AM FW_New-Horscnated       0       Merch node 2       192:168:10.81       53       DNS (t       51/2       MILCNT_sede node 2       192:168:10.81       53       DNS (t       51/2       S1/2       S1/2<	6	TCP/9192					9192	192.168.10.14	Allow	53703	192.168.10.68	Mercnt node 1	ъ	FW_New-IPsec-VPN-Connection	/23/2023 02:54:00 AM
1/1/23/2023 02:54:02 AM Connection Progress         MILCNT_sede node 2         192:168:10.36         538         DNS (t           1/1/23/2023 02:54:02 AM Connection Progress         0         Bresont node 2         192:168:10.44         53         DNS (t           1/1/23/2023 02:54:02 AM FW_Packet-Discarded         0         Bresont node 2         192:168:10.44         53         DNS (t           1/1/23/2023 02:54:02 AM Connection_Allowed         0         Mercnt node 1         192:168:10.18         52097         Allow 192:168:10.12         53         192:168:20.18         542:4         192:168:20.125         53         DNS (t           1/1/23/2023 02:54:02 AM FW_New-Pisc-VPN-Connection         0         Mercnt node 1         192:168:01.65         53/303         Allow 192:168:10.14         51/92         TCPI9'1           1/1/23/2023 02:54:03 AM Connection_Interface_Changed         0         MILCNT_sede node 1         192:168:01.15         58/87         192:168:0.08         54/33         192:168:0.15         53/81         192:168:0.89         54/3         HTTPS	6	HTTPS	443	2.168.20.89	23781 1	192.168.20.15	443	192.168.10.89		58878	192.168.10.15	MILCNT_sede node 1	ъ	Connection_Interface_Changed	/23/2023 02:54:00 AM
1/12/32/2023 02:54:02 AM FW_Packet-Discarded         0         Bresont node 2         192:168.10.40         4453         192:168.10.21         53           1/12/32/2023 02:54:02 AM FW_Packet-Discarded         0         Mercnt node 2         192:168.10.40         4453         192:168.10.21         53           1/12/32/2023 02:54:02 AM Connection_Allowed         0         Mercnt node 2         192:168.10.81         52097         Allow         192:168.10.125         53         192:168.20.18         58424         192:168.20.125         53         DNS (L           1/12/32/2023 02:54:03 AM FW_New-Pasec-VPN-Connection         0         Mercut node 1         192:168.10.61         53/303         Allow         192:168.10.14         5192         172:2168.20.15         53/371         172:172:172:172:172:172:172:172:172:172:	6	HTTPS	443	2.168.20.52	23781 1	192.168.20.51	443	192.168.10.52		58878	192.168.10.51	MILCNT_sede node 1	10	Sample_Critical_Event	/23/2023 02:54:00 AM
1/1/23/2023 02:54:02 AM Connection_Allowed 🕏 Mercnt node 2 192.168 10.18 52097 Allow 192.168.10.125 53 192.168.20.18 58424 192.168.20.125 53 DNS (t 1/1/23/2023 02:54:03 AM FW_New-IPsec-VPN-Connection 5 Mercnt node 1 192.168.10.68 53703 Allow 192.168.10.14 5192 TCP/91 1/1/23/2023 02:54:03 AM Connection_Interface_Changed 5 MILCNT_sede node 1 192.168.10.15 58878 192.168.10.89 443 192.168.20.15 53781 192.168.20.89 443 HTTPS	P) 17	DNS (UDP)					53	192.168.10.145		63861	192.168.10.36	MILCNT_sede node 2	Ð	Connection_Progress	/23/2023 02:54:02 AM
1/12/32/023 0/2:54:03 AM FW_New-IPsec-VPN-Connection 😈 Mercnt node 1 192.168.10.68 53703 Allow 192.168.10.14 5192 TOP91 1/12/32/023 0/2:54:03 AM Connection_Interface_Changed 5 MILCNT_sede node 1 192.168.10.15 58878 192.168.10.89 443 192.168.20.15 5/3761 192.168.20.89 443 HTTPS	17						53	192.168.10.21		4453	192.168.10.40	Brescnt node 2	0	FW_Packet-Discarded	/23/2023 02:54:02 AM
1/1/23/2023 02:54:03 AM Connection_Interface_Changed 🐧 MILCNT_sede node 1 192:168:10.15 58878 192:168.10.89 443 192:168:20.15 538781 192:168:20.89 443 HTTPS	P) 17	DNS (UDP)	53	2.168.20.125	38424 1	192.168.20.18	53	192.168.10.125	Allow	52097	192.168.10.18	Mercnt node 2	ъ	Connection_Allowed	/23/2023 02:54:02 AM
	6	TCP/9192					9192	192.168.10.14	Allow	53703	192.168.10.68	Mercnt node 1	ъ	FW_New-IPsec-VPN-Connection	/23/2023 02:54:03 AM
14/22/00/23 03:64-02 AM Comple Critical Event NO MILCHT and and 4 100 100 10 61 50070 100 10 50 50 50 50 50 50 50 50 50 50 50 50 50	6	HTTPS	443	2.168.20.89	23781 1	192.168.20.15	443	192.168.10.89		58878	192.168.10.15	MILCNT_sede node 1	ъ	Connection_Interface_Changed	/23/2023 02:54:03 AM
71/23/2023 02:34:03 AMI Sample_Childar_Event 10 MilCold_selle node 1 132:106.10.51 58616 132:106.10.52 443 132:106:20.51 23/81 132:106:20.52 443	6	HTTPS	443	2.168.20.52	23781 1	192.168.20.51	443	192.168.10.52		58878	192.168.10.51	MILCNT_sede node 1	<b>1</b> 0	Sample_Critical_Event	/23/2023 02:54:03 AM

#### 3.4 Dashboard

**Forcepoint NGFW - Events overview:** This dashlets display the different types of events like connection events, VPN events etc. logged by Forcepoint NGFW firewall.

Forcepoint NG	<b>0</b> 🗹 – 3		
dest_ip_address	log_priority	log_status	src_ip_address
192. <mark>1</mark> 68.10.14	0	fw_new-ipsec-vpn-connection	192.168.10.68
192.168.10.21	0	fw_packet-discarded	192.168.10.40
192.168.10.89	0	connection_interface_changed	192.168.10.15
192.168.10.125	0	connection_allowed	192.168.10.18
192.168.10.145	0	connection_progress	192.168.10.36

**Forcepoint NGFW - Critical events:** The dashlet will capture critical events like Malware or threat related events etc. detected by Forcepoint NGFW firewall.

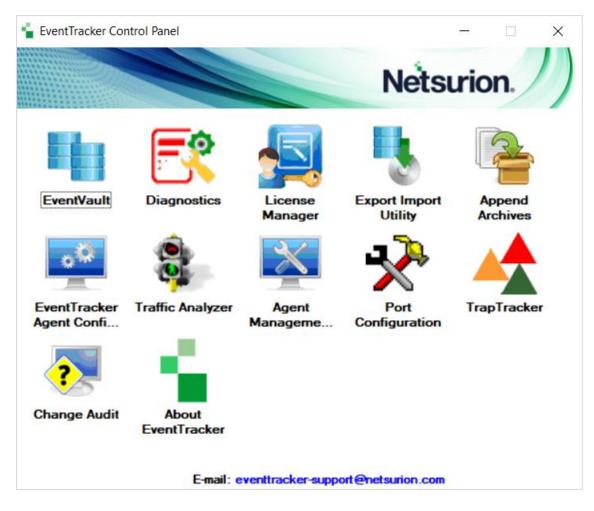




# 4 Importing Forcepoint NGFW Data Source Integration into the Netsurion Open XDR platform

Import the Data source integration items in the following sequence.

- Category
- Alerts
- Token Template
- Reports
- Knowledge Objects
- Dashboards
- 1. Launch the Netsurion Open XDR platform **Control Panel**.
- 2. Double click on Export Import Utility and click the Import tab.



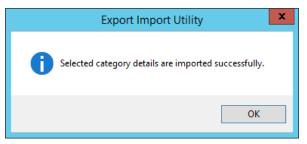


#### 4.1 Category

1. In the **Import** tab, choose the **Category** option, and then click the **Browse** button to locate the file.

🐁 Export Import Utility				_		×
Export Import						
<ol> <li>Provide the path and file nam</li> <li>Click the Import button.</li> </ol>	e of the Categorie	s file. Use the '' button to browse and loc	cate the import file.			
Options Category	Location					
◯ Filters						
<ul> <li>Alerts</li> </ul>						
O Systems and Groups		ource : /iscat				
O Token Value	L		J			
◯ Reports						
O Machine learning						
			Im	port	Clos	e

- 2. In the Browse window, locate the Categories\_ Forcepoint NGFW.iscat file and click Open.
- **3.** To import the categories, click **Import**.
- **4.** The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Category**.



5. Click **OK** or the **Close** button to complete the process.



#### 4.2 Alerts

1. In the **Import** tab, choose the **Alerts** option, and then click the **Browse** button to locate the file.

port Import			
<ol> <li>Provide the path and file</li> <li>Click the Import button.</li> </ol>	name of the Alerts file. Use the '' but	ton to browse and locate the import file.	
Options	Location		
Category	Set Active		
○ Filters	<ul> <li>Only if notifications set</li> </ul>	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on	
Alerts	O By default	"Active" key available in the configuration section.	
O Systems and Groups	Watchlist Configuration		
O Token Value	Import Watchlist configurat	ion	
<ul> <li>Reports</li> </ul>		for alerts which have Advanced watchlist configured. The user should make sure the watchlist groups are available is are imported.	
Machine learning			
	Source :		
	*.isalt		
		Import	Close

- 2. In the Browse window, locate the Alerts\_ Forcepoint NGFW.isalt file, and then click Open.
- **3.** To import the alerts, click **Import**.
- **4.** The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Alerts**.



5. Click **OK** or the **Close** button to complete the process.



#### 4.3 Token Template

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Parsing Rules.

		🔎 Admin <del>-</del>
Active Watch Lists	FAQ Tile Configuration	Manager
Alerts	Group Management	MITRE ATT&CK Rules
Casebook Configuration	Q IP Lookup Configuration	🧭 Parsing Rules
Category	Knowledge Objects	Report Settings
Diagnostics	M Machine Learning Jobs	Systems
Event Filters	👆 Machine Learning Settings	🗙 Users
Eventvault	🏓 Manage API keys	⊕ Weights

2. In the Parsing Rules interface, click the Template tab and then click Import Configuration.

			Admin / Parsing Rules
Parsing Rul	es		
Parsing Rule	Template		
Groups		<b>(+)</b>	C 1 T

3. In the Import window, click Browse to search and locate for the Templates\_Forcepoint NGFW.ettd file.





**4.** It takes few seconds to load the templates and once templates are displayed, click the appropriate template, and click **Import**.

select	ted file is: Template_Forcepoint NGFW.ettd		🖆 Browse 📱			
	Template name	Separator	Template description	Added date	Added by	Group Name
C	Forcepoint NGFW - All events	Ч	Nov 29 09:37:35 CNT01 CEF:0JFORCEPOINTJFirewalli6.8.8/70027[Sample_C ntical_Event1[0]deviceExternalId=MILANO_sede node 1 dvchost=192:10. 0.248 dvc=1921.00.248 strc=192:168.10.012 dstr=192:168.168 sp dpt=443 proto=6 deviceInboundInterface=0 act=Allow sourceTranslated Address=178 168.02.247 deviceInboundInterface=0 act=Allow sourceTranslated Address=178 168.02.047 deviceInboundInterface=0 act=Allow sourceTranslated Address=178 168.02.047 deviceInboundInterface=0 act=Allow sourceTranslated Port=23781 destinationTranslatedPort=443 deviceFacility= Packet Filtering rt=Nvor 29 2022 15:3742 app=HTTPS out=3670 in=7788 sc11abel=R4leD  cs1=1682 cc21abel=N4RtMedled cs2=16332		ETAdmin	Forcepoint NGFV

5. The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Template.** 

#### 4.4 Reports

1. In the **Import** tab, choose the **Reports** option and then click **New (\*.etcrx)**.

port Import		
<ol><li>Click the Import button</li></ol>	me of Schedule Report file. Use the '' button to browse and locate the import file.	
Options Category Filters Alerts Systems and Groups Token Value Reports Machine learning	Location O Legacy (*issch) O Legacy (*issch) Source : *issch	
	Incont	llose

2. In the **Reports Import** window, click **Select file** to locate **Reports\_ Forcepoint NGFW.etcrx** file.



3. Select the check box of all the files and click the **Import**  $\mathbb{T}$  button to import the selected files.

🖕 Reports Imp	ort					>
Note : If report(s)	) contains template, first import template	and proceed with report import process.				
Select file C:	\Users\ETAdmin\Desktop\Forcepoint	NGFW\Report_Forcepoint Firewall.etcrx		Select file		
Available reports						
Title		Frequency Show all	- Q Q			
	Title	Sites	Groups	Systems	Frequen	су
	orcepoint NGFW - Events overview				Undefined	
<						>
Note: Set run 1	time option is not applicable for Defined	Reports and Hourly Reports				
			nutes Set			
Replace	to	F	Replace Assign systems			
			Note: Make sure that Site(s	), Group(s) and System(s) selections are v	alid.	$\otimes$

**4.** The Netsurion Open XDR platform displays a success message on successfully importing the selected file in **Reports**.

Export Import Utility	x
Selected reports configurations are imported successfully	
ОК	

5. Click **OK** or the **Close** button to complete the process.



#### 4.5 Knowledge Objects (KO)

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Knowledge Objects.

🗏 Netsurion.		🐥 Admin <del>v</del>	Tools 🗸 🌔 🗸
Active Watch Lists	FAQ Tile Configuration	MITRE ATT&CK Rules	/ Dashboard / Home
Alerts	Group Management	Detection Rules	
Casebook Configuration	🔍 IP Lookup Configuration	🧭 Parsing Rules	
Category	Knowledge Objects	🖉 Report Settings	
Collection Point	M Machine Learning Jobs	Systems	
1 Diagnostics	👆 Machine Learning Settings	Q Users	
Event Filters	🏓 Manage API keys		ution brief document
Eventvault	Manager		ution brief document

2. In the Knowledge Objects interface, click the Import  $\blacksquare$  button to import the KO files.

	Knowledge Objects					
Q 	Search objects	Objects 🕀 📳 🏦 🌣				
	Groups	+ 🖉 🗓		Î		
C Cytance						
	EventTracker					

**3.** In the **Import** window, click **Browse** and locate the **KO\_Forcepoint NGFW.etko** file, and then click **Upload** to upload the file.

Import					×
Select file			🚰 Browse	Upload	
					Close



4. Select the check box next to the browsed KO file and then click the  $\mathbb{F}$  Import button.

Impo			×
Sele	ect file		🗁 Browse Upload
	Object name	Applies to	Group name
<	Forcepoint NGFW	Firewall NGFW v6.8.8 and later	Forcepoint Firewall
			Import Close

5. The Netsurion Open XDR platform displays a successful message on successfully importing the selected file in **Knowledge Objects**.

File imported su	ccessfully.
	ОК

6. Click **OK** or the **Close** button to complete the process.



#### 4.6 Dashboard

1. Log in to the Netsurion Open XDR platform and go to Dashboard > My Dashboard.

	Netsurion.		🐥 Admin 🗸 Tools 🗸 🌔 🗸
	Home		📌 / Dashboard / Home
Q Dasl	hboard , Dashboard	_	
à	Threats		0
	Incidents	entry point	Indicators of Compromise USB activities, New services or software install
	MITRE ATT&CK®		
	Machine Learning		Solution brief document PCI DSS v3.2 Solution brief document

2. In the My Dashboard interface, click the Import  $\mathbb{T}$  button to import the dashlet files.

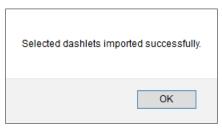
≡	Netsurion	Ļ	Admin <del>-</del>	Tools <del>-</del>	••
	My Dashboard		🔶 / Dashb	oard / My D	ashboard
٩			<b>(+)</b>	9 <b>* 1</b>	<b>T</b> ?
~	Windows				~

- 3. In the Import window, click Browse to locate the Dashboards\_Forcepoint NGFW.etwd file and then click Upload.
- 4. Click the **Select All** checkbox to select all the dashlet files and click **Import** to import the selected dashlet files.

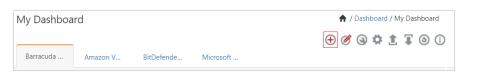
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.					
			🗁 В	rowse	Upload
Available widgets					
Select All					
Forcepoint NGFW - Ev	ents 🔽 Forcenoù	at NGEW - Critica			
- rorcepoint worw Ex	ents — Forcepon	it ivoi w - critica			
		it ivor w - critica			
	ents — Forcepon	it Nor w - chuca			
		it nor w - chica.			
		it nor w - chitta.			
	ents — Forcepoin	n norw - chica.			
	ents — Forcepoin	n norw - chica.			
	ents Erotepon	n norw - chica.			
	ents — Forcepoin	n norw - chica.			



5. The Netsurion Open XDR platform displays the success message on successfully importing the dashlet files.



6. Then, in the **My Dashboard** interface click the **Add**  $\oplus$  button to add the dashboard.



7. In the Add Dashboard interface, specify the Title and Description and click Save.

Edit Dashboard	
Title	
Forcepoint NGFW	
Description	
Applies to Forcepoint NGFW firewall v6.8.8 and above	
	Save Delete Cancel

- From the newly created dashboard interface (for example, Forcepoint NGFW), click the Configuration Sutton to add the Forcepoint NGFW dashlets.
- 9. Search and select the newly imported dashlets and click Add.

Customize dashlets	×
Forcepoint NGFW	Q
Forcepoint NGFW - Critical eve Forcepoint NGFW - Events over	



# 5 Verifying Forcepoint NGFW Data Source Integration in the Netsurion Open XDR platform

#### 5.1 Category

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Category.

	Netsurion,		🐥 Admin 🗸	Tools 🗸 🌔 🗸
=	Active Watch Lists	FAQ Tile Configuration	MITRE ATT&CK Rules	/ Dashboard / Home
q	Alerts	Group Management	Detection Rules	
	Casebook Configuration	Q IP Lookup Configuration	🧭 Parsing Rules	
	Category	• Knowledge Objects	Report Settings	
	Collection Point	M Machine Learning Jobs	Systems	
	Diagnostics	🗞 Machine Learning Settings	🕰 Users	
	Event Filters	🔎 Manage API keys	The Weights	ution brief document
	Eventvault	Manager		ution brief document

2. In the **Category** interface, under the **Category Tree** tab, click the **Forcepoint NGFW** group folder to expand and see the imported categories.

Category	
Category Tree	Search
Forcep	oint NGFW rcepoint NGFW - Events overview



#### 5.2 Alerts

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Alerts.

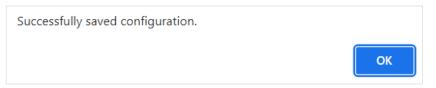
≡	Netsurion		🐥 Admin <del>-</del>	Tools 🗸 🌔 🗸
	Active Watch Lists	FAQ Tile Configuration	MITRE ATT&CK Rules	/ Dashboard / Home
q	Alerts	Group Management	Detection Rules	
	Casebook Configuration	Q IP Lookup Configuration	🕖 Parsing Rules	
~	Category	Knowledge Objects	Report Settings	
	Collection Point	M Machine Learning Jobs	Systems	
	Diagnostics	👆 Machine Learning Settings	🛱 Users	
	Event Filters	🔎 Manage API keys	H Weights	ution brief document
	Eventvault	Manager		ution brief document

In the Alerts interface, type Forcepoint NGFW in the Search field and click the Search button.
 The Alerts interface will display all the imported Forcepoint NGFW alerts.

Ð	Activate Now	Click 'Activate Now' after making all changes		
		Alert Name 🔨		
✓ 옪슈 Forcepoint Firewall: Critical events detected				

**3.** To activate the imported alert, toggle the **Active** button, which is available next to the respective alert name.

Once done, it displays a success message on successfully configuring the alerts.



4. Click **OK** and click **Activate now** to activate the alerts after making the required changes.

#### Note

You can modify the required alert separately, and select the respective alert name check box, and then click **Activate Now** to save the alert modifications.

#### Note

In the Alert Configuration interface, specify the appropriate System for better performance.



#### 5.3 Token Template

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Parsing Rules.

		🔎 Admin <del>-</del>
Active Watch Lists	FAQ Tile Configuration	Manager
▲ Alerts	Group Management	MITRE ATT&CK Rules
Casebook Configuration	Q IP Lookup Configuration	🧭 Parsing Rules
Category	Knowledge Objects	Report Settings
Diagnostics	M Machine Learning Jobs	Systems
Event Filters	👆 Machine Learning Settings	QQ Users
Eventvault	🔎 Manage API keys	

2. Go to the **Template** tab and click the **Forcepoint NGFW** group folder to view the imported Token template.

Group : Fo	rcepoint NGFW	Search	Q				Сİ
Template I	Name Template D	escription	Added By	Added Date	Active		
Forcepoint	NGFW - All events Applies to F above	prcepoint NGFW v6.8.8 and	Akash	Jan 19 06:10:13 AM		Ø	

#### 5.4 Reports

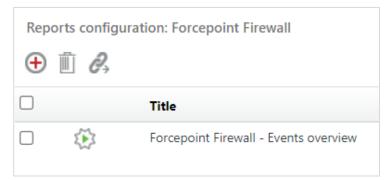
1. In the Netsurion Open XDR platform, click the Reports menu, and then click Report Configuration.

≡	Netsurion.			<b>A</b>	Admin <del>v</del>
	My Dashboard				🕈 / Dashboa
Q					⊕ @
à	Report Configuration				
	Report Dashboard	tion			
	Explorer	: In	c – x	Windows-New So	chedule

- 2. In the Reports Configuration interface, select the Defined option.
- **3.** In the search field, type **Forcepoint NGFW** and click **Search** to search for the Forcepoint NGFW reports.



4. The Netsurion Open XDR platform displays the reports for Forcepoint NGFW.

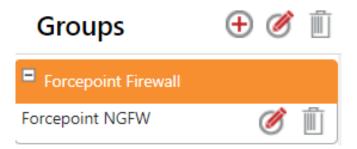


#### 5.5 Knowledge Objects (KO)

1. In the Netsurion Open XDR platform, hover over the Admin menu and click Knowledge Objects.

E Netsurion		. ▲ Admin <del>-</del>	Tools 🗸 🌔 🗸
Active Watch Lists	FAQ Tile Configuration	MITRE ATT&CK Rules	/ Dashboard / Home
Alerts	Group Management	Detection Rules	
Casebook Configuration	🔍 IP Lookup Configuration	🧭 Parsing Rules	
Category	Knowledge Objects	Report Settings	
Collection Point	M Machine Learning Jobs	Systems	
Diagnostics	👆 Machine Learning Settings	🙁 Users	
Event Filters	🄎 Manage API keys	H Weights	ution brief document
Eventvault	Manager		ution brief document

2. In the Knowledge Object interface, under Groups tree, click the Forcepoint NGFW group to expand and view the imported Knowledge objects.



3. Click Activate Now to apply the imported Knowledge Objects.



#### 5.6 Dashboard

In the Netsurion Open XDR platform, go to Home > My Dashboard, and click the Customize dashlets
 button.



- 2. In the **Customize dashlets** interface, search for **Forcepoint NGFW** in the search field.
- **3.** The following Forcepoint NGFW dashlet files will get displayed.

Customize dashlets		×
Forcepoint NGFW		Q
✓ Forcepoint NGFW - Critical eve	✓ Forcepoint NGFW - Events over	
		Add Delete Close



#### **About Netsurion**

Netsurion<sup>®</sup> delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at <u>netsurion.com</u>.

# Contact Us

Corporate Headquarters

Netsurion Trade Centre South 100 W. Cypress Creek Rd Suite 530 Fort Lauderdale, FL 33309

#### **Contact Numbers**

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1		
MSP Enterprise <u>SOC-MSP@Netsurion.com</u>		1 (877) 333-1433 Option 1, Option 2		
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3		
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4		

https://www.netsurion.com/eventtracker-support