

# Integrate pfSense *EventTracker Enterprise*

Publication Date: Jul.18, 2016

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://www.eventtracker.com)

# Abstract

This guide provides instructions to configure **pfSense** to send the syslog events to EventTracker Enterprise.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.x and later, and pfSense 2.3.1.

## Audience

Administrators, who are responsible for monitoring **pfSense** using EventTracker Enterprise.

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

*This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems 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 Prism Microsystems, 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.*

*© 2016 Prism Microsystems Corporation. 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
Introduction .....	3
Pre-requisites.....	3
Integration Method for pfSense.....	3
EventTracker Knowledge Pack (KP).....	6
Categories .....	6
Alerts.....	6
Flex Reports .....	6
Import pfSense knowledge pack into EventTracker .....	7
Category .....	8
Alerts.....	10
Templates .....	11
Knowledge Object.....	12
Flex Reports.....	13
Verify pfSense knowledge pack in EventTracker .....	14
Category .....	14
Alerts.....	14
Template .....	15
Knowledge Object.....	16
Flex Reports.....	17
Create Flex Dashboards in EventTracker .....	17
Schedule Reports.....	17
Create Dashlets.....	20
Sample Flex Dashboards.....	24

# Introduction

**pfSense** is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a physical computer or a virtual machine to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. pfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint.

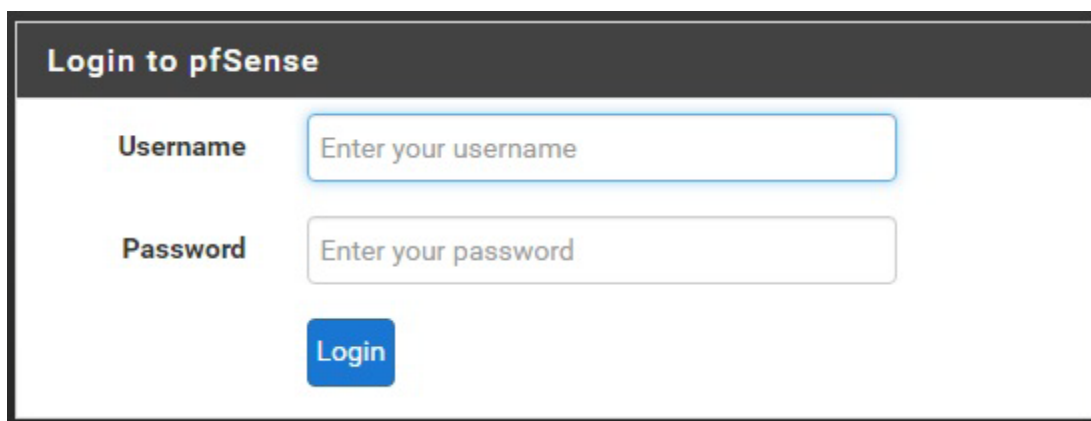
EventTracker collects the logs, helps administrator to analyze the events and generate the reports for the defined firewall rules and monitors the configured alerts.

## Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- pfSense version 2.3.1 must be installed and configured.

## Integration Method for pfSense

1. Log into the pfSense Web interface.



The image shows a screenshot of the pfSense web interface login page. At the top, there is a dark header with the text "Login to pfSense" in white. Below the header, there are two input fields. The first is labeled "Username" and contains the placeholder text "Enter your username". The second is labeled "Password" and contains the placeholder text "Enter your password". Below these fields is a blue button with the text "Login" in white.

Figure 1

2. Go to **Status** -> **System Logs**

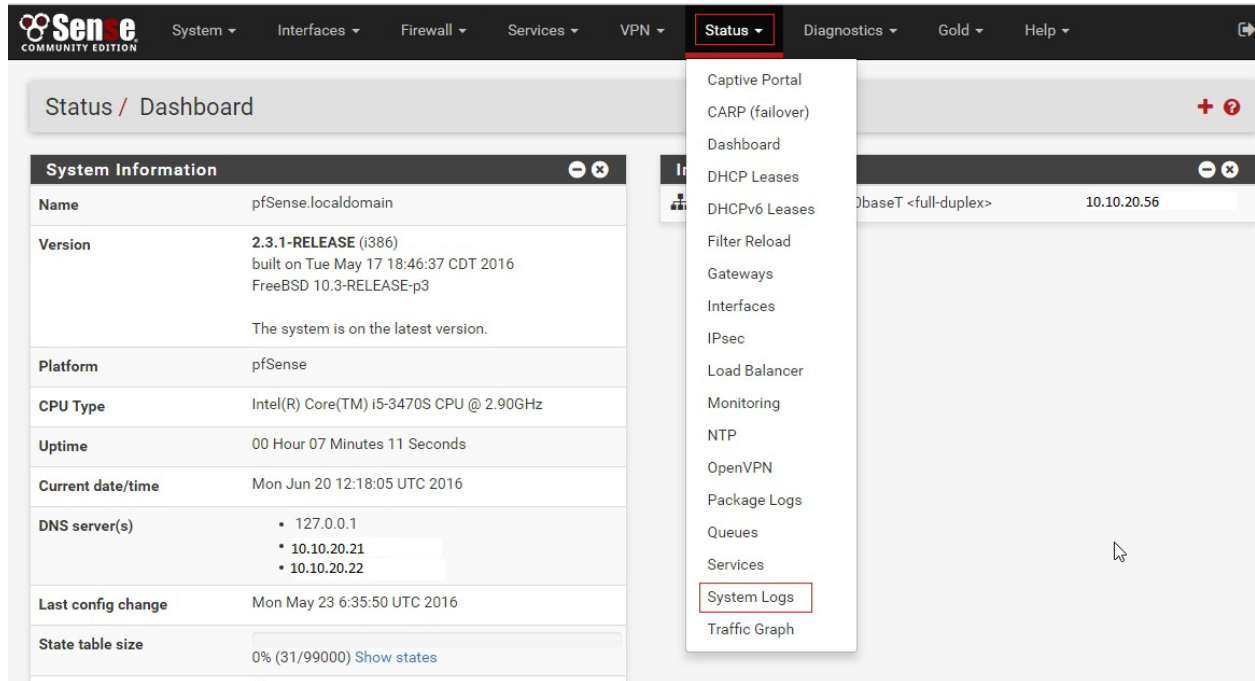


Figure 2

3. Click the **Settings** tab.



Figure 3

4. Enable the checkbox "Enable syslogging to remote syslog server".

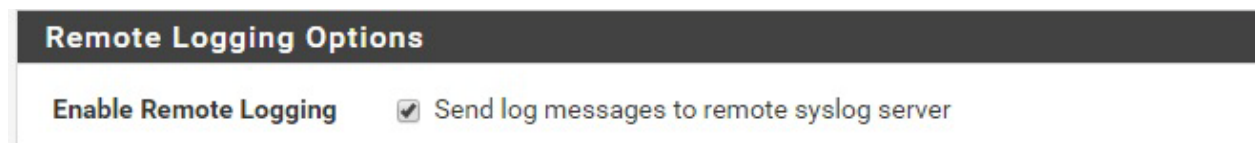


Figure 4

**NOTE:**

**Source Address:** Chooses which interface on pfSense to use for initiating log messages. If the target syslog server is across an IPsec tunnel, this should be a local interface address inside of a Phase 2 definition for the IPsec tunnel.

**IP Protocol:** Selects IPv4 or IPv6 to be used for sending log messages when multiple possibilities exist.

**Enable Remote Logging:** When checked, send syslog entries to the defined servers.

**Remote Syslog Servers:** List of remote syslog servers. It can be an IP address (IPv4 or IPv6), hostname, or IP: port if syslog is on a non-default port. (E.g. EventTracker manager IP address and port (10.150.26.33:514))

**Remote Syslog Contents:** Select the items which will be sent via remote syslog. **Everything** is the preferred choice.

5. Type the IP of the logging server in the box next to Remote syslog server i.e. EventTracker manager.
6. Check the boxes for the log entries to forward.

**Remote Logging Options**

Source Address: Default (any) ▼  
This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If you pick a single IP, remote syslog servers must all be of that IP type. If you wish to mix IPv4 and IPv6 remote syslog servers, you must bind to all interfaces.  
NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol: IPv4 ▼  
This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Enable Remote Logging:  Send log messages to remote syslog server

Remote Syslog Servers

Server 1: 10.150.26.33:514  
Server 2:   
Server 3:   
IP addresses of remote syslog servers, or an IP:port.

Remote Syslog Contents

Everything  
 System events  
 Firewall events  
 DHCP service events  
 Portal Auth events  
 VPN (PPTP, IPsec, OpenVPN) events  
 Gateway Monitor events  
 Server Load Balancer events  
 Wireless events

Save

**Note:** syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

Figure 5

7. Click Save.

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker.

The following Knowledge Packs are applicable in EventTracker v7.x and later to support pfSense.

## Categories

- **pfSense-Traffic allowed and blocked details**

This category provides information related to traffic blocked or passed by the rule configured on the firewall.

## Alerts

- **pfSense - IPsec tunnel down**

This alert is generated when IPsec tunnel goes down.

## Flex Reports

- **pfSense: Traffic allowed and blocked details**

This report provides the information related to protocols (TCP, UDP, ICMP, and ICMPv6), protocol numbers, traffic passed or blocked on the interface and direction of the traffic (inbound or outbound).

Event Time	Computer	Source IP	Source Port	Destination IP	Destination Port	Interface	Direction	Action	Protocol	Protocol Number
Jul 05 09:14:09	PFSense-FW1	fe80::6155:9317:a929:7941		ff02::1		em1	in	block	ICMPv6	
Jul 05 10:47:23	PFSense-FW1	176.250.250.176	59308	209.121.27.19	23	em0	in	block	tcp	6
Jul 05 10:47:27	PFSense-FW1	169.254.161.191	137	169.254.100.125	137	em1	in	block	udp	17
Jul 05 10:52:45	PFSense-FW1	10.12.19.108	33420	10.12.19.22	3389	em0	in	block	tcp	6
Jul 05 10:52:45	PFSense-FW1	10.12.19.108	28202	10.12.19.22	80	em0	in	pass	tcp	6
Jul 05 11:00:02	PFSense-FW1	44.13.0.23	unreachport	219.144.47.209		em0	in	block	icmp	1
Jul 05 17:20:24	PFSense-FW1	88.142.184.37	4553	209.114.49.109	23	em0	in	block	tcp	6

Figure 6

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
7/6/2016 4:56:02 PM	<a href="#">123</a>	TOM / <b>pfSense-FW1</b>	N/A	N/A	Syslog
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Jul 05 11:00:01 10.0.16.148 Jul 05 11:00:02 filterlog: 9,16777216,,1000000103,em0,match,block,in,4,0x0,,56,50935,0,none,1,icmp,81,44.13.0.23,219.144.47.209,unreachport,94.23.0.83,UDP,2701561			
7/6/2016 4:56:02 PM	<a href="#">123</a>	TOM / <b>pfSense-FW1</b>	N/A	N/A	Syslog
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Jul 05 17:43:49 10.0.16.148 Jul 05 17:42:49 filterlog: 9,16777216,,1000000103,em0,match,block,in,4,0x0,,53,41124,0,DF,6,tcp,56,199.32.94.101,219.144.47.109,48603,23,0,5,4153559790,,5440,,mss;sackOK;TS			
7/6/2016 4:56:01 PM	<a href="#">123</a>	TOM / <b>pfSense-FW1</b>	N/A	N/A	Syslog
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Jul 05 10:47:26 10.0.16.148 Jul 05 10:47:27 filterlog: 7,16777216,,1000000101,em1,match,block,in,4,0x0,,128,22544,0,none,17,udp,78,169.254.161.191,169.254.100.125,137,137,58			
7/6/2016 4:56:01 PM	<a href="#">123</a>	TOM / <b>pfSense-FW1</b>	N/A	N/A	Syslog
<b>Event Type:</b> Information <b>Log Type:</b> Application <b>Category Id:</b> 0		<b>Description:</b> Jul 05 17:35:55 10.0.16.148 Jul 05 17:34:55 filterlog: 5,16777216,,1000000003,em1,match,block,in,6,0x00,0x00000,255,ICMPv6,58,32,fe80::7c0b:6cb:399f:e7c2,ff02::1			

Figure 7

# Import pfSense knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence

- Categories
- Alerts
- Templates
- Knowledge Objects
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**.



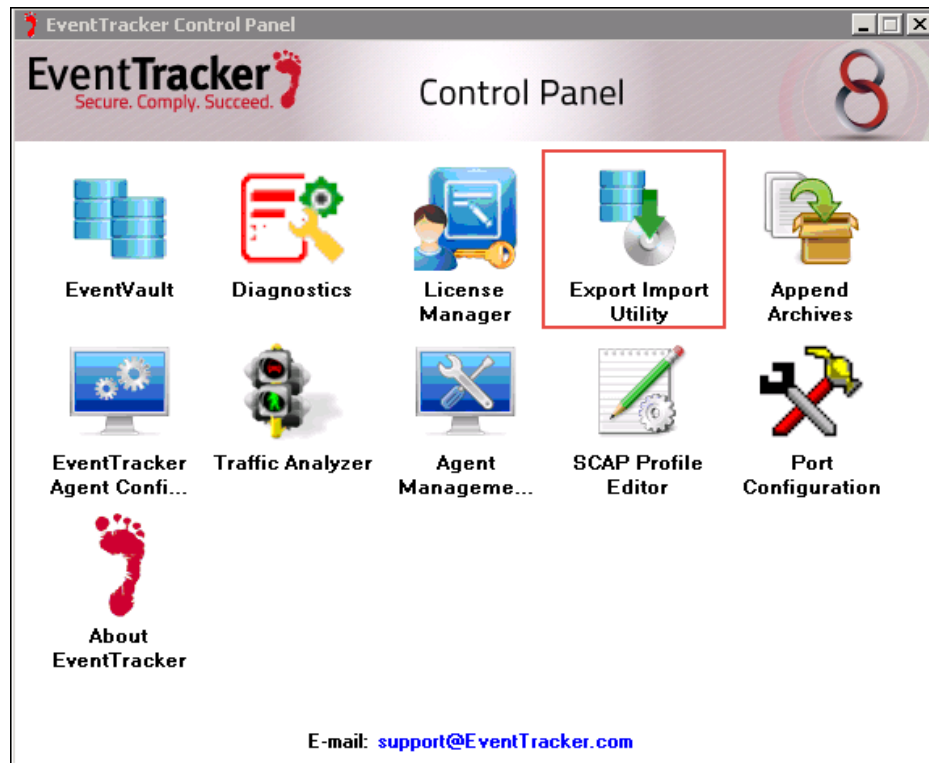



Figure 8

3. Click the **Import** tab.
4. **Import knowledge pack as specified in the sequence.**

## Category

1. Click **Category** option, and then click the browse  button.
2. Locate the **All pfSense group of categories.iscat** file, and then click **Open** button.

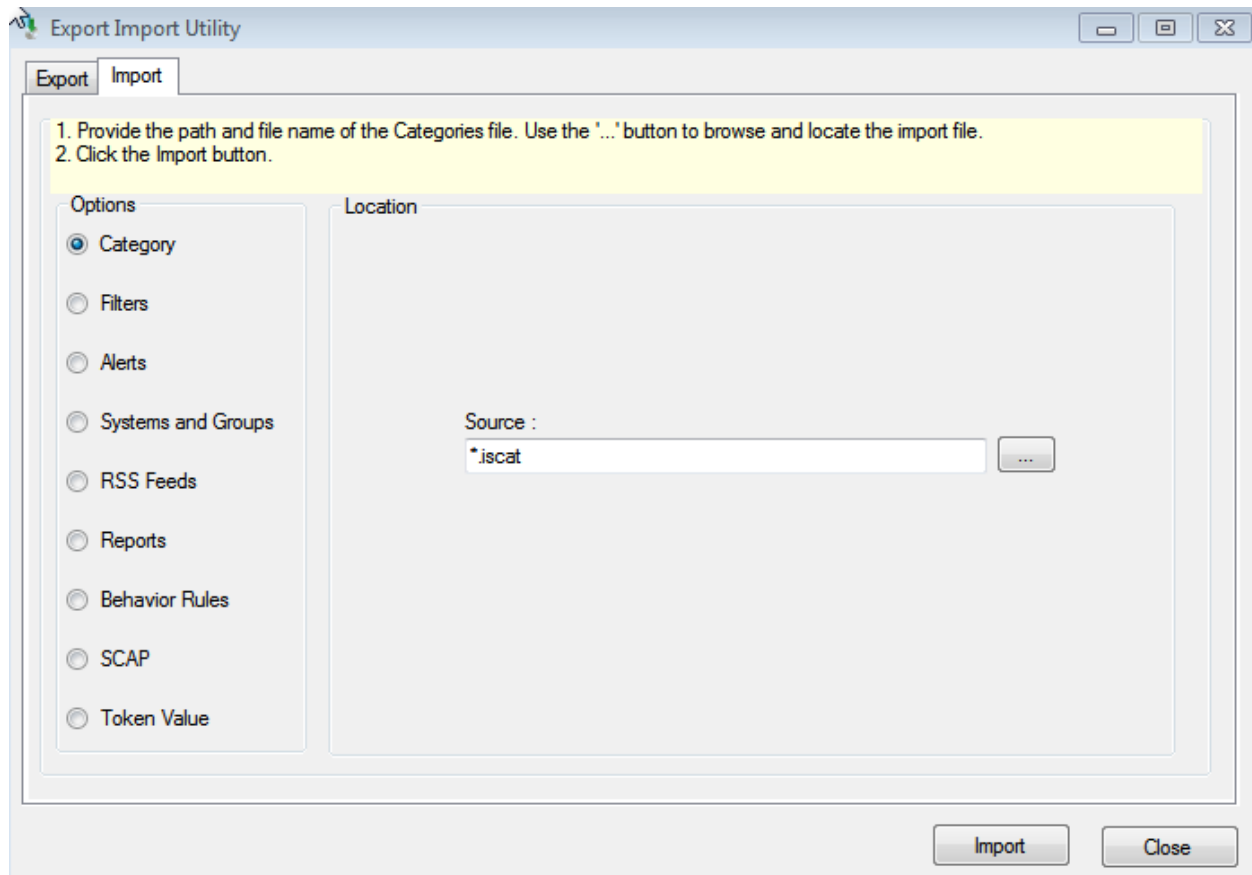


Figure 9

3. To import categories, click the **Import** button.

EventTracker displays success message.

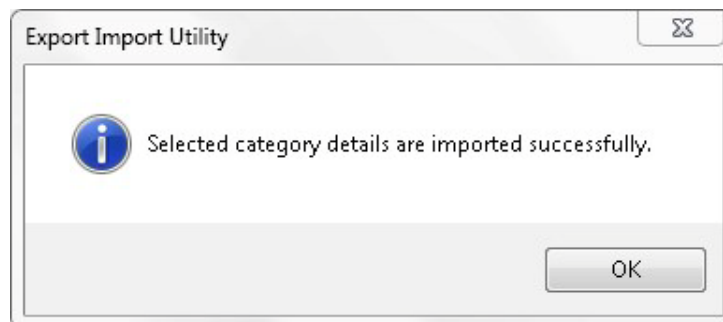



Figure 10

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

## Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **All pfSense group of alerts.isalt** file, and then click the **Open** button.

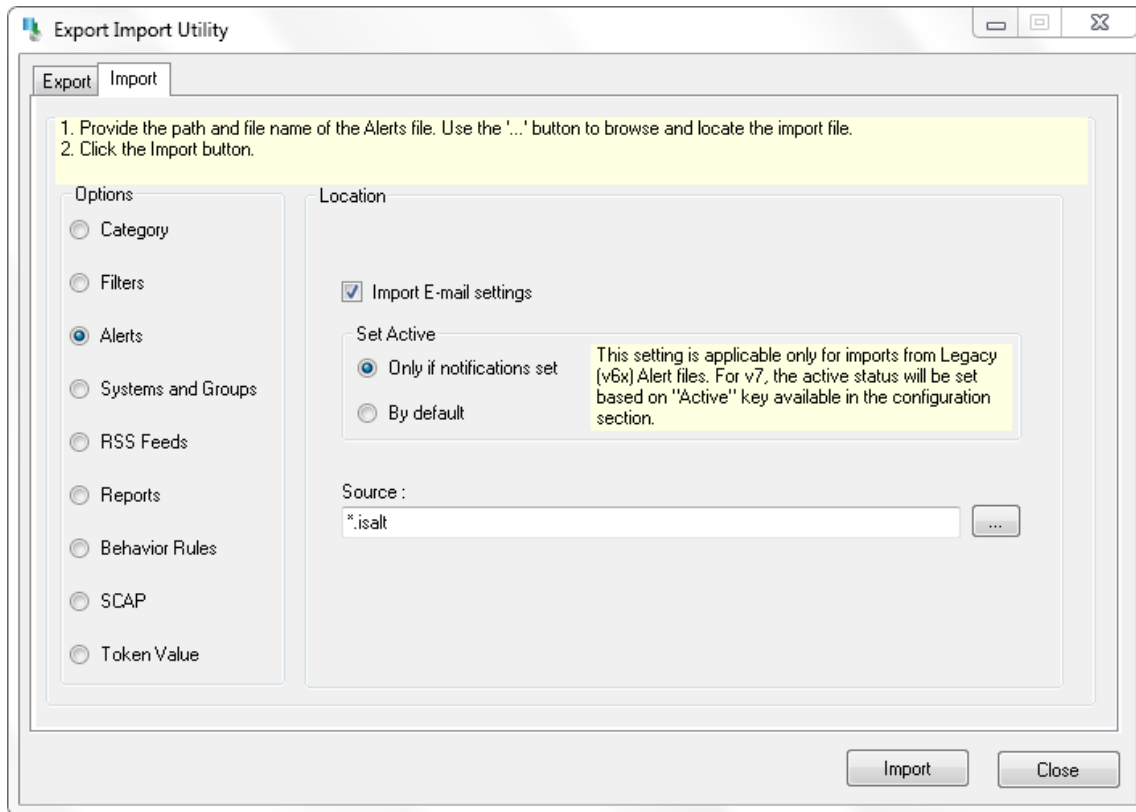


Figure 11

3. To import alerts, click the **Import** button.  
EventTracker displays success message.

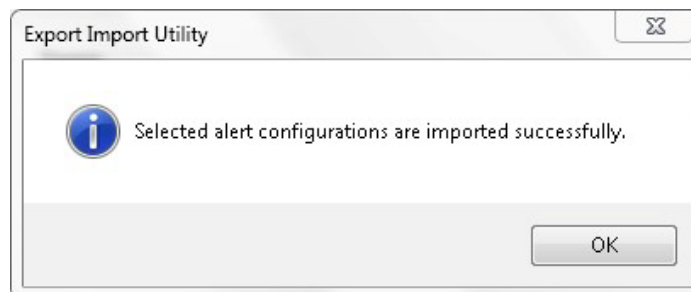



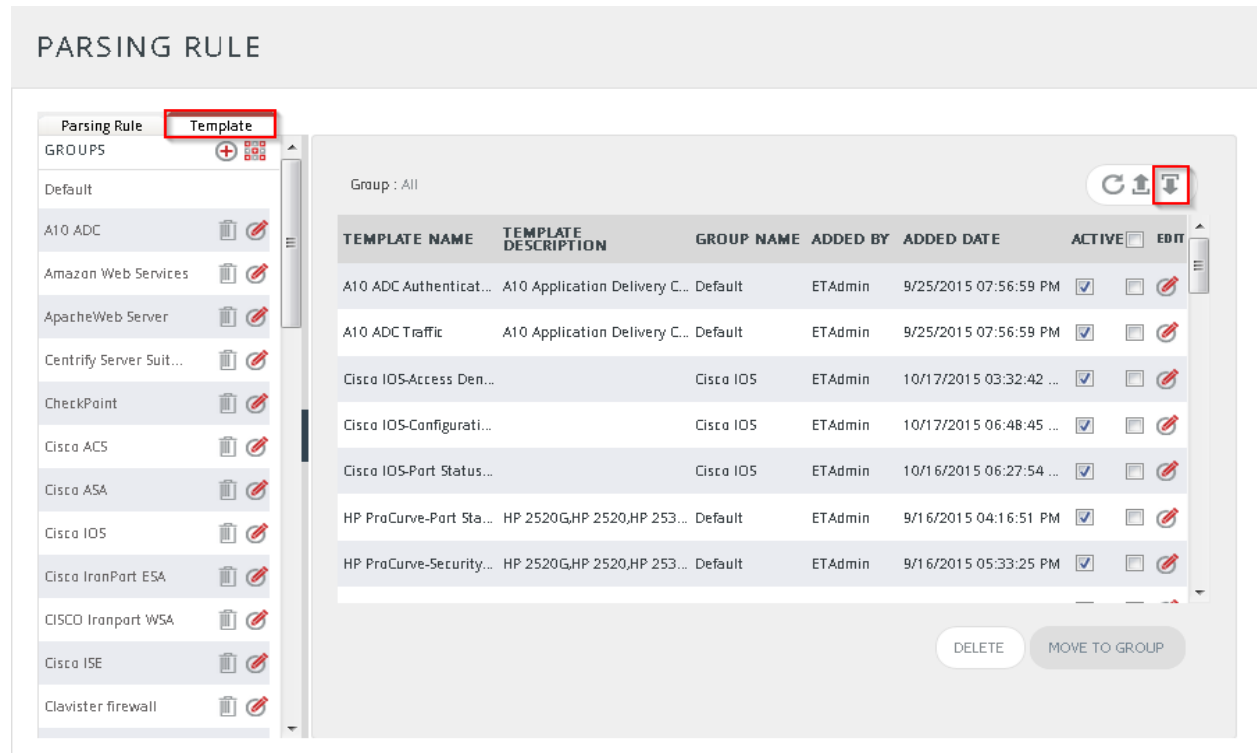
Figure 12

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

# Templates

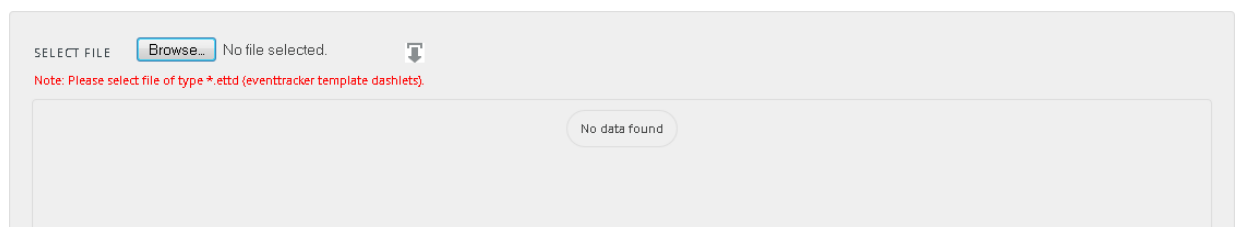
1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on  'Import' option.

PARSING RULE



TEMPLATE NAME	TEMPLATE DESCRIPTION	GROUP NAME	ADDED BY	ADDED DATE	ACTIVE	EDIT
A10 ADC Authentica...	A10 Application Delivery C...	Default	ETAdmin	9/25/2015 07:56:59 PM	<input checked="" type="checkbox"/>	
A10 ADC Traffic	A10 Application Delivery C...	Default	ETAdmin	9/25/2015 07:56:59 PM	<input checked="" type="checkbox"/>	
Cisco IOS-Access Den...		Cisco IOS	ETAdmin	10/17/2015 03:32:42 ...	<input checked="" type="checkbox"/>	
Cisco IOS-Configurati...		Cisco IOS	ETAdmin	10/17/2015 06:48:45 ...	<input checked="" type="checkbox"/>	
Cisco IOS-Part Status...		Cisco IOS	ETAdmin	10/16/2015 06:27:54 ...	<input checked="" type="checkbox"/>	
HP ProCurve-Part Sta...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 04:16:51 PM	<input checked="" type="checkbox"/>	
HP ProCurve-Security...	HP 2520G,HP 2520,HP 253...	Default	ETAdmin	9/16/2015 05:33:25 PM	<input checked="" type="checkbox"/>	

Figure 13



SELECT FILE  No file selected.

Note: Please select file of type \*.ettd (eventtracker template dashlets).

No data found

Figure 14

3. Locate the **All pfSense group of templates.ettd** file, and then click the **Open** button.

SELECTED FILE IS: All pfSense group of templates.ettd

TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/> pfSense:Traffic allowed and blocked details	\n	Jul 05 17:43:49 10.0.16.148 Jul 05 17:42:49 filterlog: 9,16777216,,1000000103,e m0,match,block,in,4,0x0,,53,41124,0,DF,6,tcp,56,179.32.94.101,209.124.47.10 9,48603,23,0,5,4153559790,,5440,,mss:sackOK;TS	7/6/2016 4:14:03 PM	ETAdmin	pfSense

Figure 15

4. To import tokens, click the **Import** button.

EventTracker displays success message.

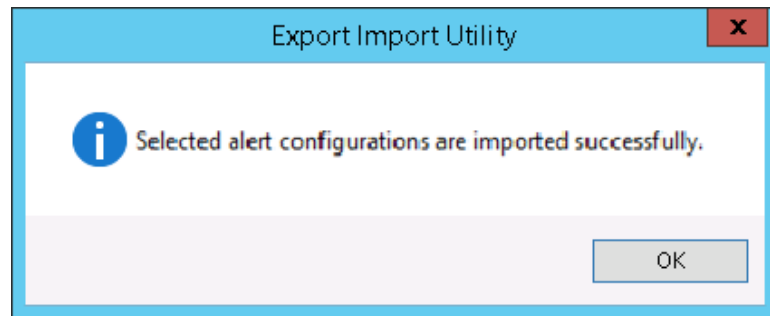


Figure 16

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

## Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on **Import** option.



Figure 19

3. In **IMPORT** pane click on **Browse** button.

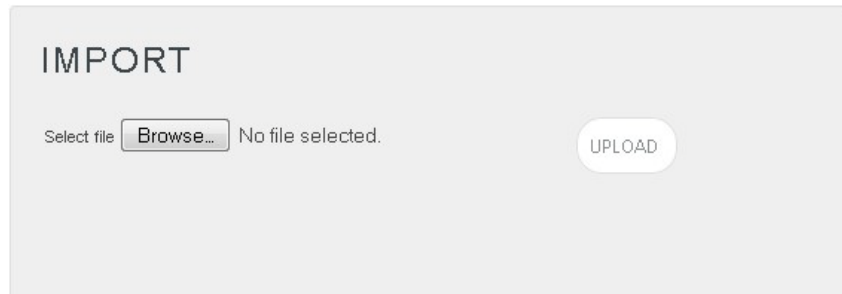


Figure 20

4. Locate **All pfSense group of knowledge object.etko** file, and then click the **UPLOAD** button.

## Flex Reports

1. Click **Report** option, and then click the browse  button
2. Locate the **All pfSense group of flex reports.issch** file, and then click the **Open** button.

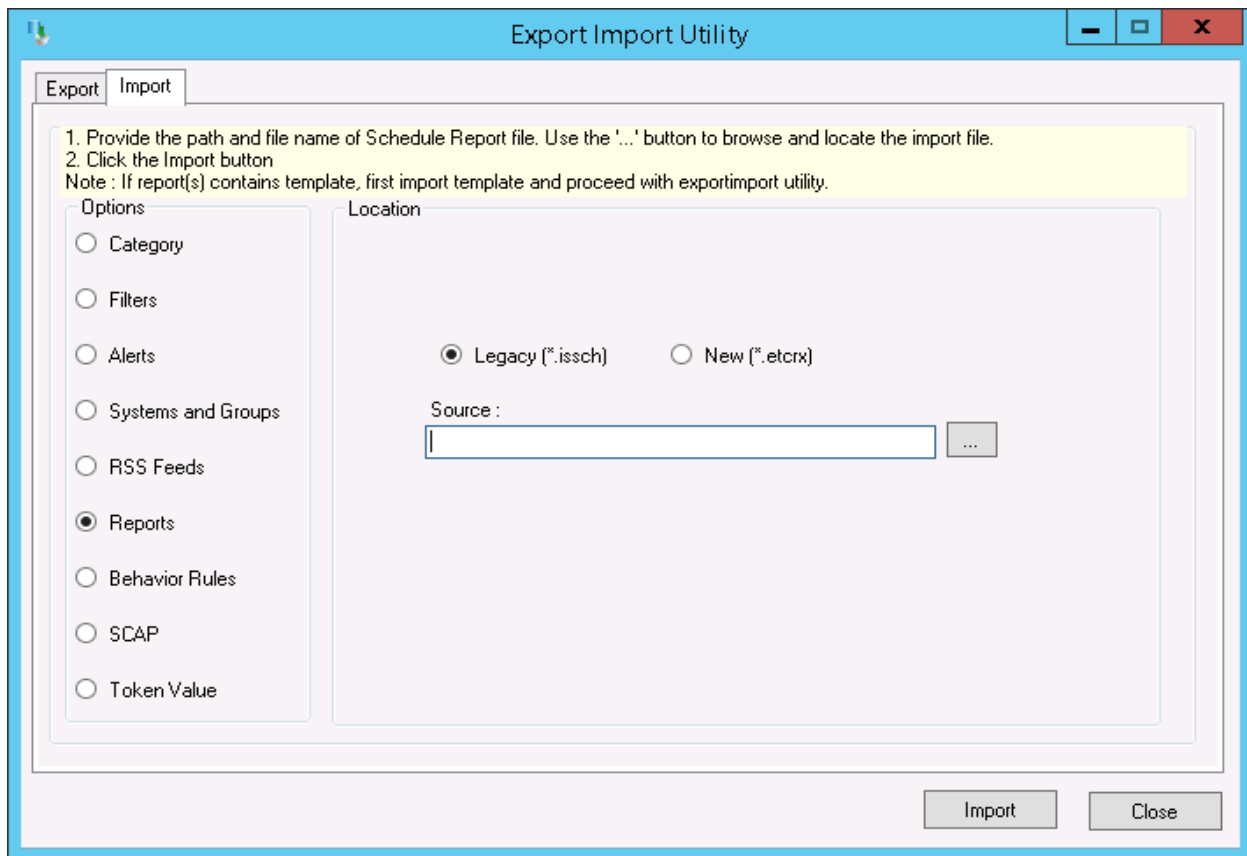


Figure 17

3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.

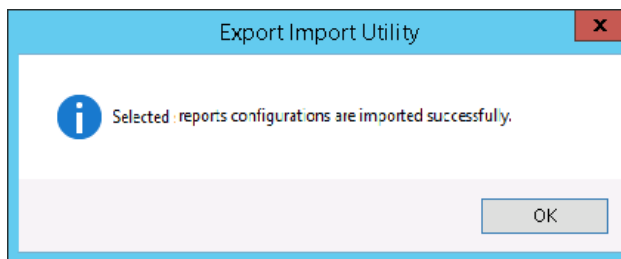


Figure 18

## Verify pfSense knowledge pack in EventTracker

### Category

1. In the **EventTracker Enterprise**, web interface.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, expand **pfSense** group folder to see the imported categories.



Figure 21

### Alerts

1. In the **EventTracker Enterprise**, web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type '**pfSense**', and then click **Go** button.

Alert Management page will display all imported **pfSense** alert.

ALERT MANAGEMENT

Search by Alert name pfSense

ACTIVATE NOW Click 'Activate Now' after making all changes Total: 1 Page Size 25

ALERT NAME ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/> PfSense: IPSec tunnel down	<input type="checkbox"/> Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	PfSense 2.3.1

DELETED

Figure 22

- To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

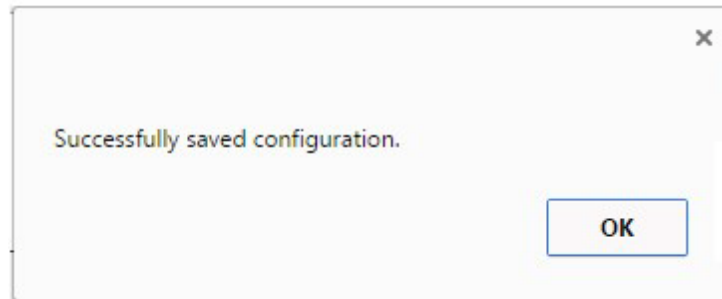


Figure 23

- Click the **OK** button, and then click the **Activate now** button.

**NOTE:**

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

## Template

- Logon to **EventTracker Enterprise**.
- Click the **Admin** menu, and then click **Parsing Rules**.



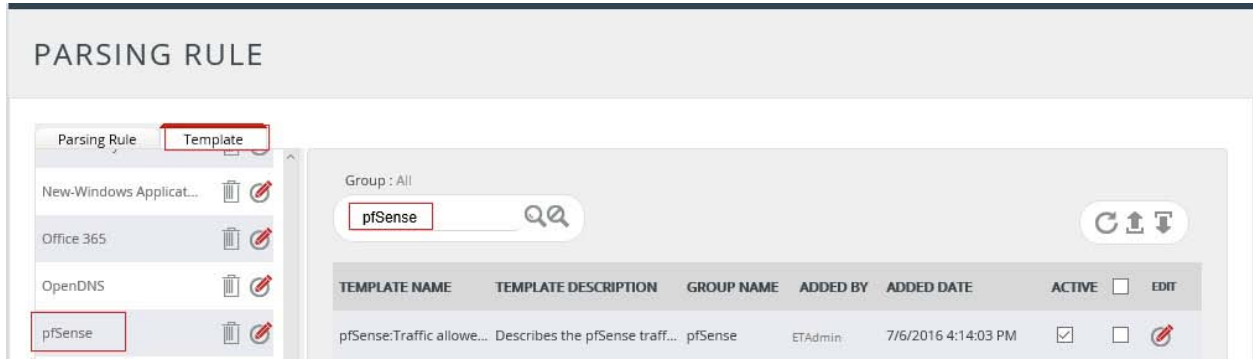


Figure 24

## Knowledge Object

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Scroll down and select **pfSense** in **Objects** pane. Imported **pfSense** object details are shown.

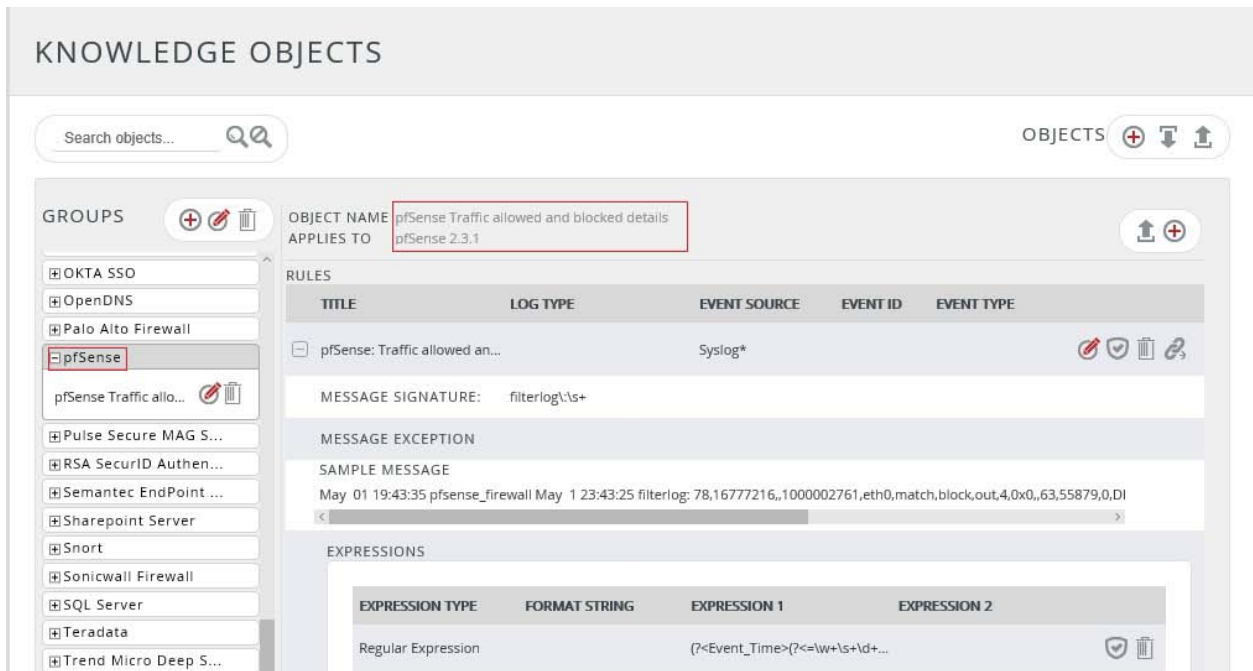


Figure 25

## Flex Reports

1. In the **EventTracker Enterprise**, web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.

EventTracker displays **Defined** page.

3. In search box enter '**pfSense**', and then click the **Search** button.  
EventTracker displays Flex reports of **pfSense**



Figure 26

## Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise V8.0.

### Schedule Reports

1. Open **EventTracker** in browser and logon.

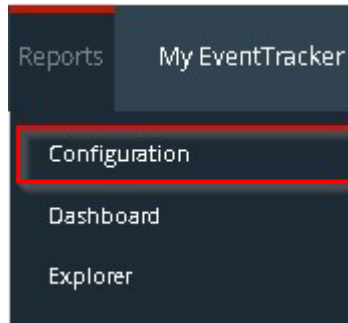



Figure 27

2. Navigate to **Reports>Configuration**.



Figure 28

3. Select **pfSense** in report groups. Check **Defined** dialog box.
4. Click on 'schedule'  to plan a report for later execution.

## REPORT WIZARD

CANCEL < BACK NEXT >

TITLE: **PFSENSE-TRAFFIC ALLOWED AND BLOCKED DETAILS**

LOGS

Review cost details and configure the publishing options. Step 8 of 10

### DISK COST ANALYSIS

Estimated time for completion: 00:00:34(HH:MM:SS)  
Number of cab(s) to be processed: 2  
Available disk space: 256 GB  
Required disk space: 50 MB

Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)

Deliver results via E-mail  
 Notify results via E-mail

To E-mail:  [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

Persist data in Eventvault Explorer

Figure 29

REPORT WIZARD

TITLE: PFSENSE-TRAFFIC ALLOWED AND BLOCKED DETAILS  
DATA PERSIST DETAIL

SELECT columns to persist

Step 9 of 10

RETENTION SETTING

Retention period: 7 days

Persist in database only [Reports will not be published and will only be stored in the respective database]

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Event Time	<input checked="" type="checkbox"/>
Computer	<input checked="" type="checkbox"/>
Source IP	<input checked="" type="checkbox"/>
Source Port	<input checked="" type="checkbox"/>
Destination IP	<input checked="" type="checkbox"/>
Destination Port	<input checked="" type="checkbox"/>

Figure 30

5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.
6. Proceed to next step and click **Schedule** button.
7. Wait till the reports get generated.

## Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

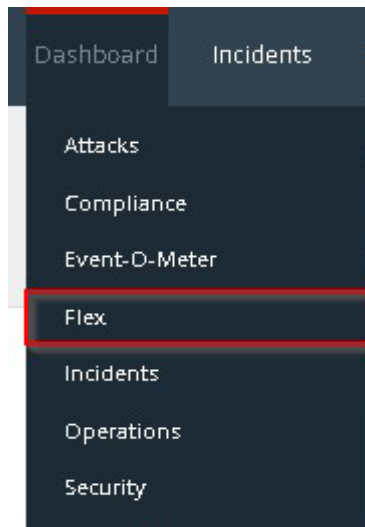


Figure 31

2. Navigate to **Dashboard>Flex**.  
Flex Dashboard pane is shown.

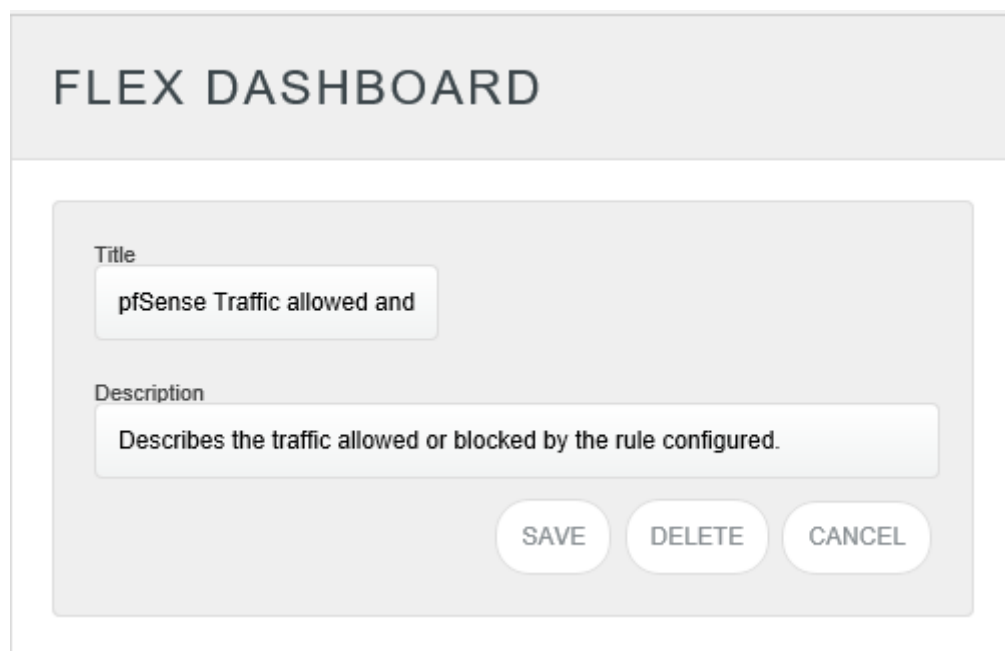



Figure 32

3. Fill suitable title and description and click **Save** button.
4. Click  to configure a new flex dashlet. Widget configuration pane is shown.

### WIDGET CONFIGURATION

WIDGET TITLE		NOTE	
<input type="text" value="pfSense: Traffic blocked by IPs"/>		<input type="text"/>	
DATA SOURCE			
<input type="text" value="pfSense-Traffic allowed and blocked details"/>			
CHART TYPE	DURATION	VALUE FIELD SETTING	AS OF
<input type="text" value="Donut"/>	<input type="text" value="1 Week"/>	<input type="text" value="COUNT"/>	<input type="text" value="Now"/>
AXIS LABELS [X-AXIS]	LABEL TEXT		
<input type="text" value="Source IP"/>	<input type="text" value="Source IP"/>		
VALUES [Y-AXIS]	VALUE TEXT		
<input type="text" value="Select column"/>	<input type="text"/>		
FILTER	FILTER VALUES		
<input type="text" value="Action"/>	<input type="text" value="block"/>		
LEGEND [SERIES]	SELECT		
<input type="text" value="Select column"/>	<input type="text" value="All"/>		

Figure 33

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

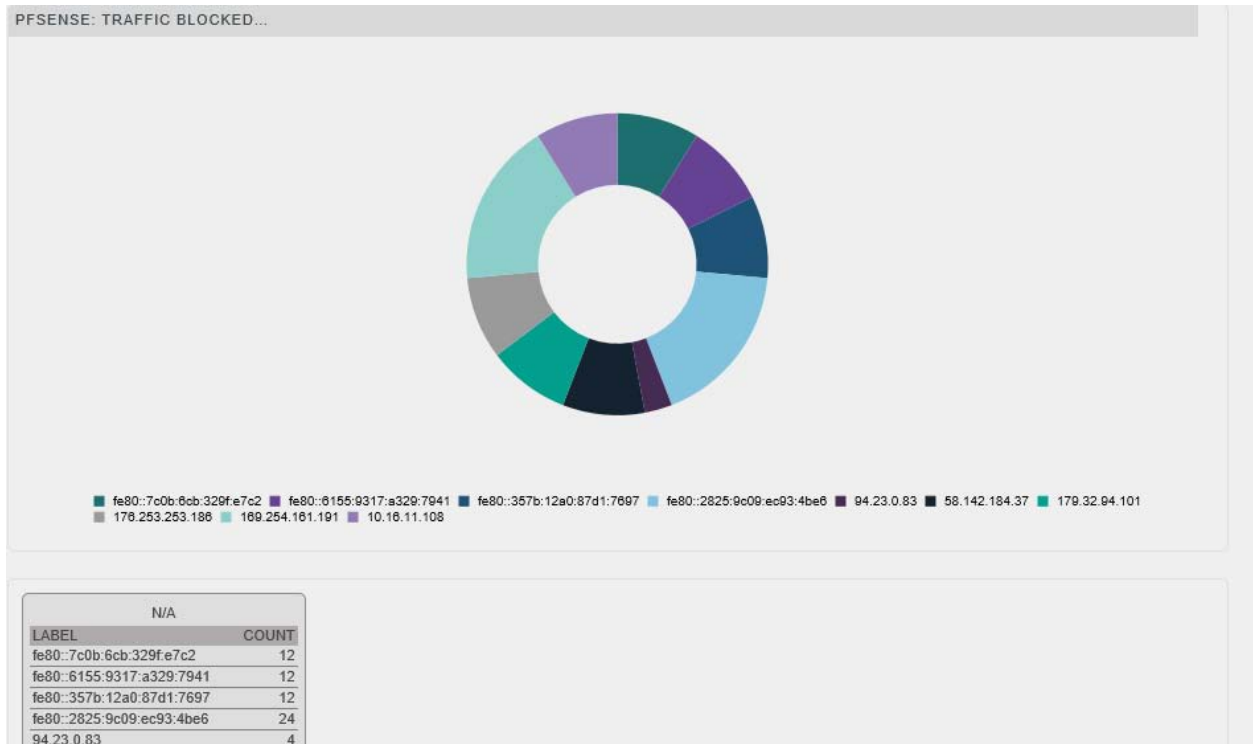




Figure 34

14. If satisfied, click **Configure** button.



Figure 35

15. Click 'customize'  to locate and choose created dashlet.

16. Click  to add dashlet to earlier created dashboard.



# Sample Flex Dashboards

For below dashboard **DATA SOURCE: pfSense: Traffic allowed and blocked details**

## 1. pfSense: Traffic blocked by IPs

**WIDGET TITLE:** Traffic blocked by IPs

**CHART TYPE:** Donut

**AXIS LABELS [X-AXIS]:** Source IP

**Label Text:** Source IP

**FILTER:** Action

**FILTER Values:** block

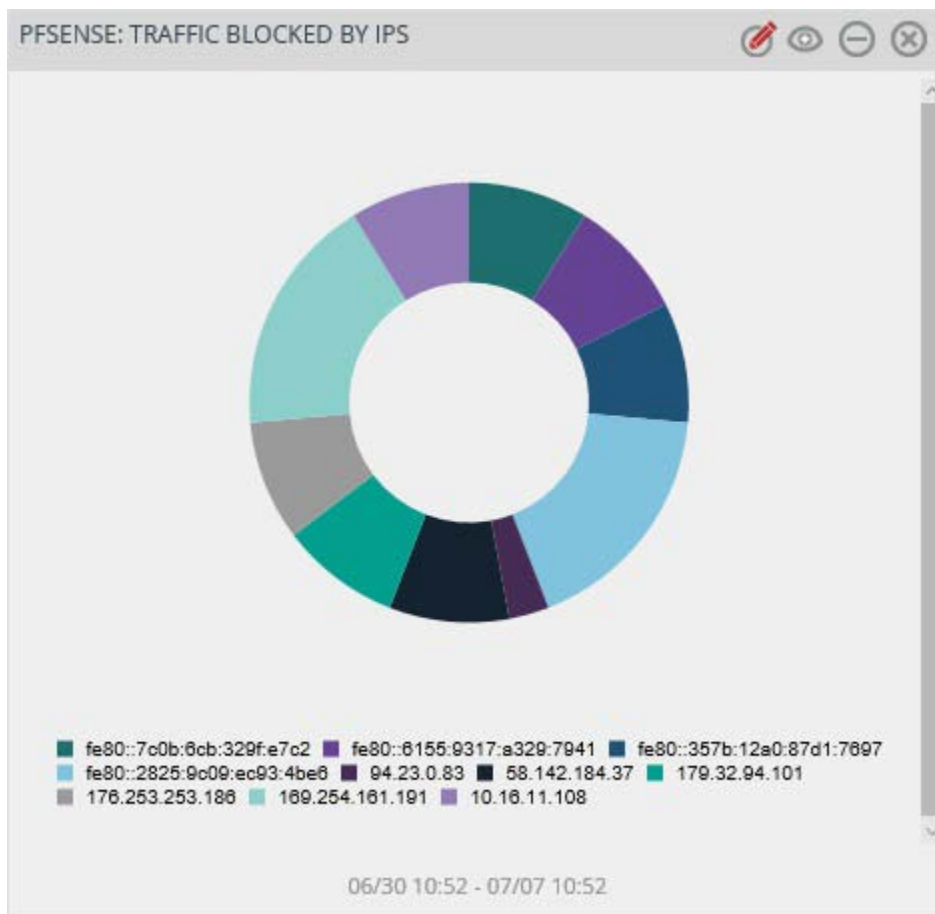


Figure 36

## 2. pfSense: Traffic blocked by Port

**WIDGET TITLE:** Traffic blocked by Port  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Destination Port  
**Label Text:** Destination Port  
**FILTER:** Action  
**FILTER Values:** block

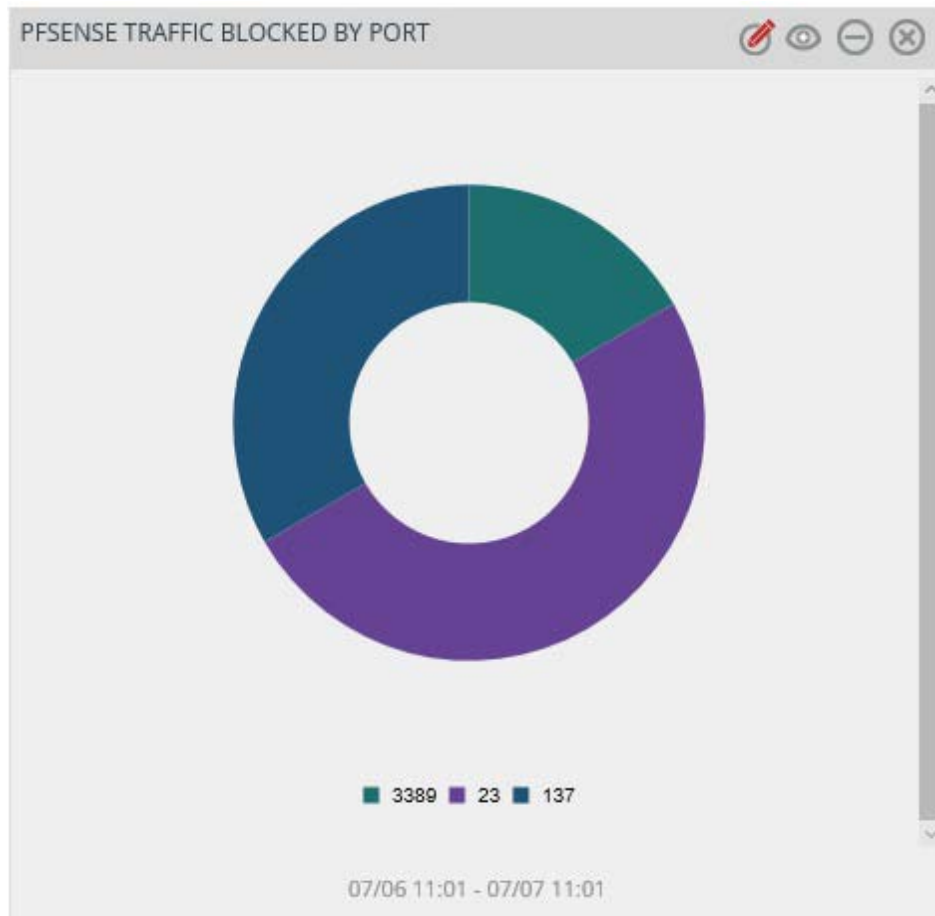


Figure 37

## 3. pfSense: Traffic blocked by Protocols

**WIDGET TITLE:** Traffic blocked by Protocols  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Protocol  
**Label Text:** Protocols  
**FILTER:** Action  
**FILTER Values:** block

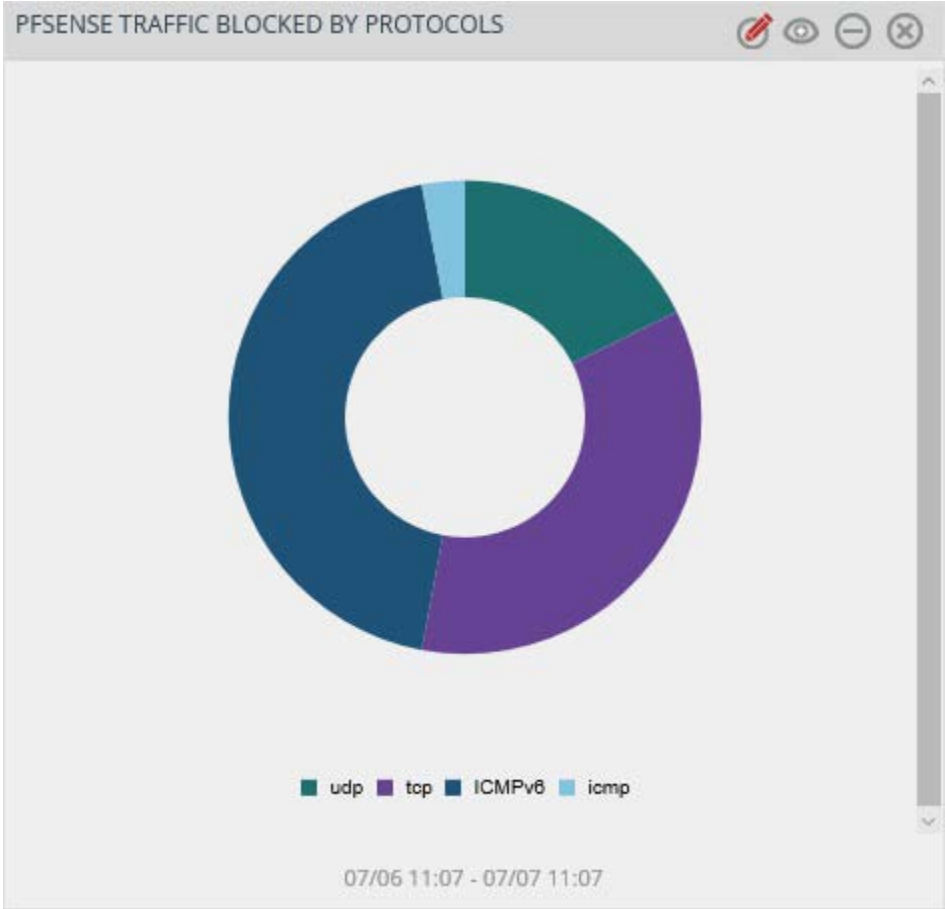


Figure 38

#### 4. pfSense: Traffic blocked by Interface

**WIDGET TITLE:** Traffic blocked by Interface

**CHART TYPE:** Donut

**AXIS LABELS [X-AXIS]:** Interface

**Label Text:** Interface

**FILTER:** Action

**FILTER Values:** block

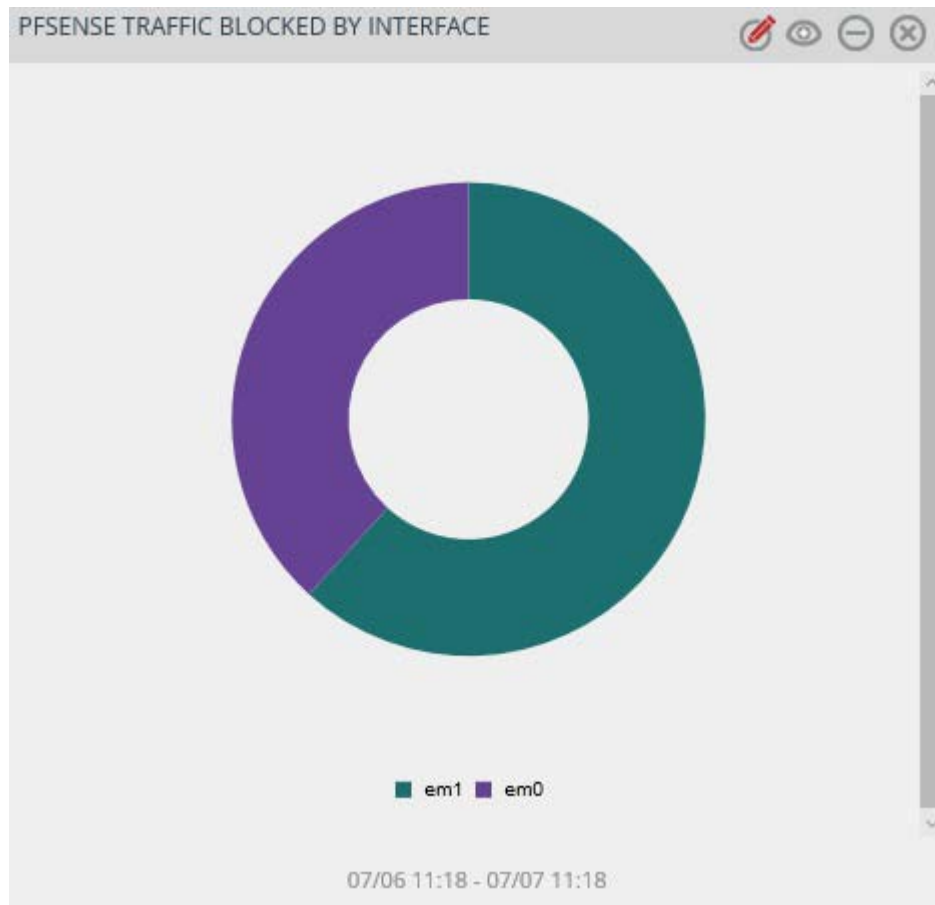


Figure 39

## 5. pfSense: Traffic allowed by IPs

**WIDGET TITLE:** Traffic allowed by IPs

**CHART TYPE:** Donut

**AXIS LABELS [X-AXIS]:** Source IP

**Label Text:** Source IP

**FILTER:** Action

**FILTER Values:** Pass

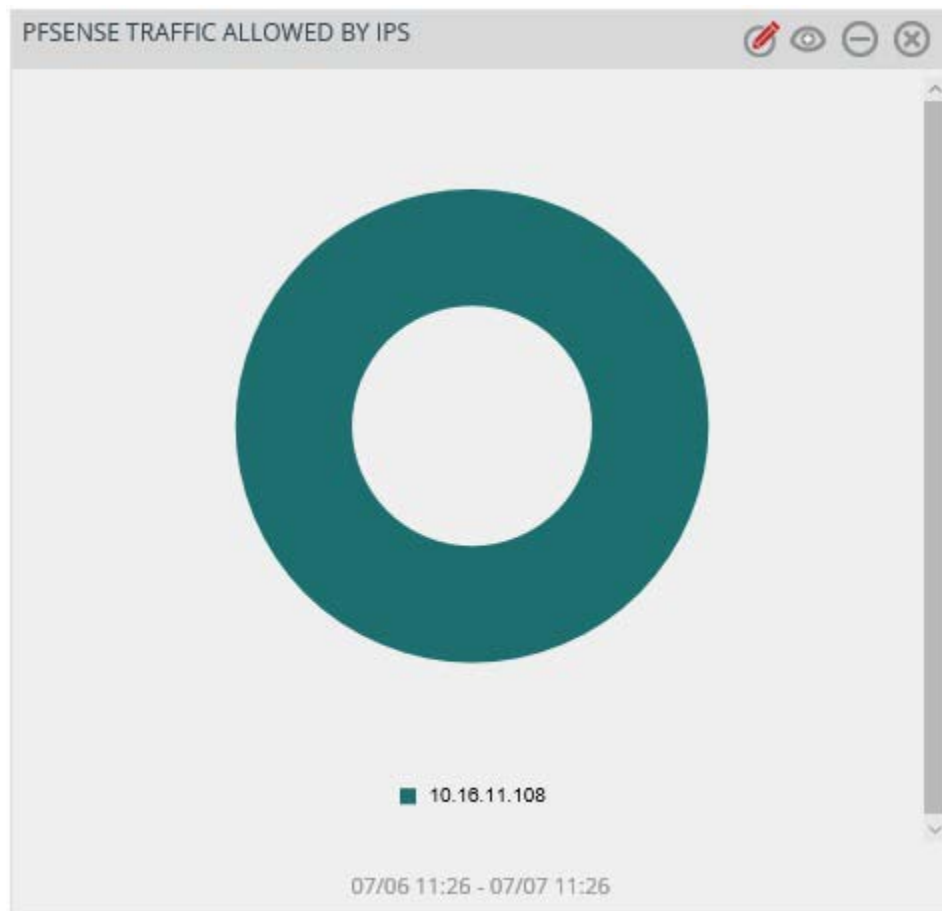


Figure 40