

**Integration Guide**

# **Integrate Sophos Firewall with EventTracker**

**EventTracker v9.2 and later**

**Publication Date:**

April 9, 2021

## Abstract

This guide provides instructions to configure Sophos UTM /SG and XG Firewall to send crucial events to EventTracker by means of syslog.

## Scope

The configuration details in this guide are consistent with EventTracker version 9.2x and later, and Sophos XG Firewall version 15.x-17.x and Sophos SG/UTM 9 and later.

## Audience

Sophos UTM/SG and XG Firewall users, who wish to forward its events to EventTracker Manager and monitor them using EventTracker.

## Table of Contents

Table of Contents	3
1 Overview	4
2 Prerequisites	4
3 Integrating EventTracker with Sophos SG/UTM and XG Firewall	4
3.1 Enabling syslog forwarding in Sophos SG/UTM firewall	4
3.2 Enabling syslog forwarding in Sophos XG firewall	5
4 EventTracker Knowledge Pack	8
4.1 Category	8
4.2 Alerts	9
4.3 Reports	9
4.4 Dashboards	19
5. Importing Sophos Firewall Knowledge Pack into EventTracker	22
5.1 Category	23
5.2 Token template	23
5.3 Knowledge Object	24
5.4 Report	26
5.5 Dashboards	27
6. Verifying Sophos Firewall Knowledge Pack in EventTracker	30
5.6 Category	30
5.7 Token templates	31
5.8 Knowledge Object	32
5.9 Report	32
5.10 Dashboards	33
About Netsurion	34
Contact Us	34

## 1 Overview

**Sophos Firewall** combines the best of both Sophos and Cyberoam technology delivering an unprecedented level of innovation to next-generation firewalls. With all new user interface, new security heartbeat technology, and a powerful new unified policy model, it introduces many important innovations that take simplicity, protection, and performance, to a whole new level. Sophos Firewall OS runs on all existing Sophos SG Series and Cyberoam NG Series hardware and is available for a variety of virtual platforms or as a software appliance.

EventTracker collects and analyses firewall events and notifies an administrator about security violations, user behavior, and traffic anomalies.

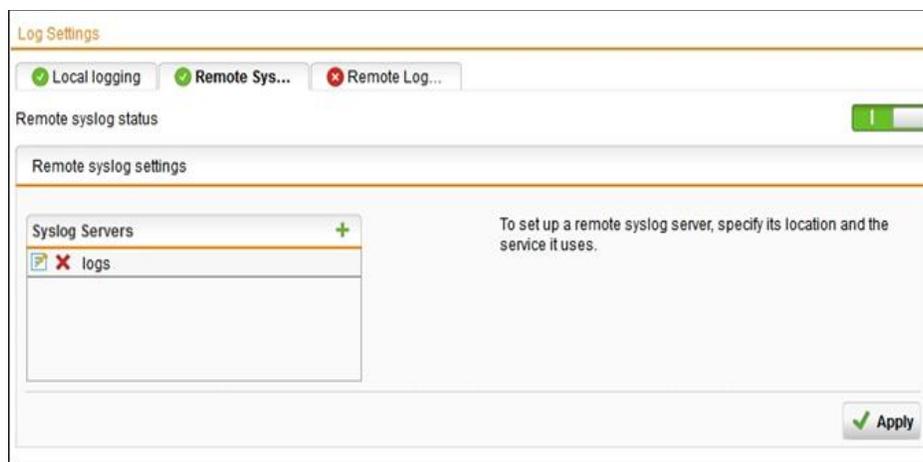
## 2 Prerequisites

- **EventTracker 9.2x and above** should be installed.
- **Sophos UTM/SG 9 and later or XG Firewall version 15.x-17.x** should be installed and configured.

## 3 Integrating EventTracker with Sophos SG/UTM and XG Firewall

### 3.1 Enabling syslog forwarding in Sophos SG/UTM firewall

1. Logon to the WebAdmin of the SG/UTM.
2. Navigate to **Logging & Reporting > Log Settings > Remote Syslog Server**.
3. Activate the **Remote Syslog status**.
4. Configure a Syslog server by clicking on + button.
  - **Name:** Freely selectable.
  - **Server:** IP or hostname of your **EventTracker Manager IP/EventTracker syslog relay IP**.
  - **Port:** UDP **514**.
5. Click **Apply**.



If syslog messages cannot be delivered, they will be buffered, and re-sends it. By default, up to 1000 logs will be buffered.

Once syslog targets have been configured, the logs to be send via syslog must also be selected on the same screen. By default, none is selected. Select the desired logs and click **Apply**.

Remote syslog log selection

Select all Select the logs that should be sent to the remote syslog server.

- Admin notifications
- Application Control
- Boot messages
- Client Authentication
- Configuration daemon
- DHCP server
- DNS proxy
- Device agent

To determine which logs are desired, you can view complete log contents and watch logs in real-time, under **Logging & Reporting > View Log Files**.

## 3.2 Enabling syslog forwarding in Sophos XG firewall

1. Navigate to **System > System Services > Log Settings** and click **Add** under the **Syslog Servers** section.
2. Enter server details.
  - **Name**
    - Enter a unique name for the syslog server.
  - **IP Address / Domain**
    - Enter the **EventTracker Manager IP Address/EventTracker syslog relay IP**.
  - **Port**
    - Enter Port number **514**, **UDP** protocol.
  - **Facility**
    - Select syslog facility for logs to be sent to the syslog server. Facility indicates to the syslog server the source of a log such as operating system, the process, or an application. It is defined by the syslog protocol. The device supports several syslog facilities for received log.
    - In the **Severity** field, select **Information** from the dropdown options.

System Services How-To Guides Log Viewer Help admin Sophos

Traffic Shaping Settings RED Malware Protection **Log Settings** Data Anonymization Traffic Shaping Services

Name \* Syslog Server ⓘ

IP Address / Domain \* 192.168.100.22

Port \* 514

Facility \* DAEMON ▼

**Severity Level \* Information ▼**

Format \* Device Standard Format ▼

**Note:** You can configure maximum five syslog servers.

3. Click **Save**.

- Once you add the server, go to the **System > System Services > Log Settings** page and enable all those logs, which are to be sent to the syslog server in the section Log Settings.

Policy Rules	▼	<input type="checkbox"/>
Invalid Traffic	▼	<input type="checkbox"/>
Local ACLs	▼	<input type="checkbox"/>
DoS Attack	▼	<input type="checkbox"/>
Dropped ICMP Redirected Packet	▼	<input type="checkbox"/>
Dropped Source Routed Packet	▼	<input type="checkbox"/>
Dropped Fragmented Traffic	▼	<input type="checkbox"/>
MAC Filtering	▼	<input type="checkbox"/>
IP-MAC Pair Filtering	▼	<input type="checkbox"/>
IP Spoof Prevention	▼	<input type="checkbox"/>
SSL VPN Tunnel	▼	<input type="checkbox"/>
Protected Application Server	▼	<input type="checkbox"/>
Heartbeat	▼	<input type="checkbox"/>

**IPS**

Anomaly	▼	<input checked="" type="checkbox"/>
Signatures	▼	<input checked="" type="checkbox"/>

**Anti-Virus**

HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Anti-Spam**

SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Content Filtering**

Web Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Application Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Events**

Admin Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Sandbox**

Sandstorm Event	<input checked="" type="checkbox"/>
-----------------	-------------------------------------

**ATP**

ATP Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
------------	-------------------------------------	-------------------------------------

**Web Server Protection**

Web Server Protection Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>
------------------------------	-------------------------------------	--------------------------

## System Health



## 4 EventTracker Knowledge Pack

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

The following knowledge packs are available in EventTracker to support Windows.

### 4.1 Category

- **Sophos Firewall- Admin activities-** This category provides information related to all admin activities.
- **Sophos Firewall- Admin login and logout-** This category provides information related to all the admin login and logout activity.
- **Sophos Firewall- Advanced threat protection-** This category provides information related to all the threat that is detected by the Sophos Firewall.
- **Sophos Firewall- Configuration changes-** This category provides information related to configuration changes done in the Sophos Firewall.
- **Sophos Firewall- Content filtering-** This category provides information related to all the content filtering that is done by the Sophos Firewall.
- **Sophos Firewall- FTP activities-** This category provides information related to all FTP activities detected by Sophos Firewall.
- **Sophos Firewall – Traffic events-** This category provides information about all accepted/denied traffic and packets by Sophos Firewall.
- **Sophos Firewall- Login Activities-** This category provides information related to all the firewall login and logout activity.
- **Sophos Firewall- Login failed-** This category provides information related to all the firewall login failures detected.
- **Sophos Firewall- IPS attack detected-** This category provides information related to all the IPS attack that is detected by the Sophos Firewall.
- **Sophos Firewall- Sandbox activities-** This category provides information related to all the sandbox activities.
- **Sophos Firewall- Security policy events-** This category provides information related to all the security policy events.
- **Sophos Firewall- Spam detection-** This category provides information related to all the spam that is detected by the Sophos Firewall.
- **Sophos Firewall- Virus detected-** This category provides information related to all the virus that is detected by the Sophos Firewall.
- **Sophos Firewall- Web Traffic-** This category provides information related to all the web traffic related events.

- **Sophos Firewall- VPN login failures-** This category provides information related to all the VPN login failures detected.
- **Sophos Firewall- Wireless security activities -** This category provides information related to all the Wi-Fi related activities detected by Sophos Firewall.

## 4.2 Alerts

- **Sophos Firewall: Advanced Threat Protection:** This alert is generated when a threat is detected by the Sophos Firewall
- **Sophos Firewall: Firewall Configuration Changed:** This alert is generated when any configuration changes are done in Sophos Firewall.
- **Sophos Firewall: User Login Activities:** This alert is generated when any firewall login activities are detected.
- **Sophos Firewall: User Logon Failed:** This alert is generated when any firewall login failure is detected.
- **Sophos Firewall: IPS Attacks Detected on System:** This alert is generated when any IPS attack is detected by the Sophos Firewall.
- **Sophos Firewall: Virus or Spam Detected on System:** This alert is generated when any virus is detected by the Sophos Firewall.
- **Sophos Firewall: VPN User Logon Failed:** This alert is generated when any VPN login failure is detected.
- **Sophos Firewall: VPN Login and Logout:** This alert is generated when any VPN login activities are detected.
- **Sophos Firewall: Object Created Deleted or Changed:** This alert is generated when any object is created, deleted, or changed.
- **Sophos Firewall: Shell Terminal Password Changed:** This alert is generated when shell terminal password change is detected.

## 4.3 Reports

- **Sophos Firewall - Administrative Activity Report -** This report provides information related to all admin activities that is done. Report contains username, source IP, message details related to the activities performed by the admin in Sophos Firewall.

LogTime	Device Name	Log Component	User Name	Source IP Address	Priority	Status	Message Details
12/21/2017 03:43:24 PM	SG135	GUI	admin	10.20.20.15	Information	Successful	SSL VPN Policy 'RA' was added by 'admin' from '10.20.20.15' using 'GUI'
12/21/2017 03:43:24 PM	SG135	GUI	admin	10.20.20.34	Information	Successful	Log Settings were changed by 'admin' from '10.20.20.15' using 'GUI'
12/21/2017 03:43:24 PM	SG135	GUI	admin	10.20.20.22	Information	Successful	SSL VPN Policy(ies) were deleted by 'admin' from '10.20.20.15' using 'GUI'
12/21/2017 03:43:24 PM	SG135	GUI	admin	10.20.20.115	Information	Successful	40 users were imported by 'admin' from '10.20.20.15' using 'GUI' successfully
12/21/2017 03:43:24 PM	CR750IN G-XP	GUI	admin	10.198.47.71	Information	Successful	Log Settings were changed by 'admin' from '10.198.47.71' using 'GUI'

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 3:43:24 PM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:15:43 timezone="IST" device_name="CR750ING-XP" device_id=C44313350024 -P29PUA log_id=062009617502 log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" priority=Information user_name="admin" src_ip=10.198.47.71 message="Log Settings were changed by 'admin' from '10.198.47.71' using 'GUI'"			
12/21/2017 3:43:24 PM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:33 timezone="PST" device_name="SG135" device_id=SFDemo1234567890 log_id=062009617503 log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" priority=Information user_name="admin" src_ip=10.20.20.15 message="SSL VPN Policy(jes) were deleted by 'admin' from '10.20.20.15' using 'GUI'"			

- Sophos Firewall - Administrator Logon or Logoff Report** - This report provides information related to all the admin login and logout activity. Report contains username, source IP, message details containing information about login or logout activity by admin in Sophos Firewall.

LogTime	Device Name	Log Component	User Name	Source IP Address	Status	Priority	Message Details
12/21/2017 03:43:24 PM	CR750ING-XP	GUI	admin	10.198.47.71	Successful	Information	Administrator &apos;admin&apos; logged out of Web Admin Console.
12/21/2017 03:43:24 PM	CR750ING-XP	GUI	admin	10.198.47.71	Successful	Information	Administrator &apos;admin&apos; logged in via Web Admin Console.

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 3:43:24 PM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:15:50 timezone="IST" device_name="CR750ING-XP" device_id=C44313350024 -P29PUA log_id=062009617507 log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" priority=Information user_name="admin" src_ip=10.198.47.71 message="Administrator 'admin' logged in via Web Admin Console."			

- Sophos Firewall - Advanced Threat Protection Management Report** - This provides information related to all the threat that is detected by the Sophos Firewall. Report contains username, source IP, source port, destination IP, destination port, threat name, thread ID, thread type, execution path and other useful information for further analysis.

LogTime	Device Name	Log Component	Log Subtype	User Name	User Group	Source IP Address	Destination IP Address	Source Port	Destination Port	Accessed	Threat Name	Threat ID	Threat Type	Priority	Login User	Process User	Execution Path
12/21/2017 02:48:49 PM	SG135	Security Policy	Drop	stacy		10.15.45.110	77.91.166.16	5361	20480	77.91.166.16	C2/Generic-A	522D2600-3A66-4A31-A8D8-FFF8C0170F9B	Standard	Warning	ATOM10	ATAX	
12/21/2017 02:48:49 PM	CR750N G-XP	Firewall	Drop	gilbert		10.198.47.71	48.161.30.47	22623	80	48.161.30.47	C2/Generic-A	C368ACFB-7A6F-4483-9063-ABCFDA8C85F7	Standard	Warning	DXC	Rumble994	C:\Windows\BootPCAT
12/21/2017 02:48:49 PM	SG135	HTTP Proxy	Alert	kim		198.156.34.2	202.31.139.173	6173	80	http://202.31.139.173/	C2/Generic-A	BF9283BE-C043-4483-9063-F890C982AD84	Standard	Warning	CYborG	UNK54	

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 2:48:49 PM	3333	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:33 timezone="PST" device\_name="SG135" device\_id=SFDemo1234567890 | log\_id=086304418010 log\_type="ATP" log\_component="Security Policy" log\_subtype="Drop" priority=Warning protocol="TCP" src\_port=3361 dst\_port=20480 sourceip=10.20.21.159 destinationip=77.91.166.16 url=77.91.166.16 threatname=C2/Generic-A eventid=522D2600-3A66-4A31-A8D8-FFF8C0170F9B eventtype="Standard" login\_user="ATOM10" process\_user="ATAX" ep\_uid= execution\_path=""

- **Sophos Firewall - Traffic Accepted or Denied Report** - This report provides information related to all the traffic that is allowed and denied by the Sophos Firewall.

LogTime	Device Name	Log Component	Log Subtype	User Name	User Group	Source IP Address	Destination IP Address	Source Port	Destination Port	Source MAC Address	Application Name	Application Category	Application Technology	Application Risk	Priority	Status	Message Details	Packet Sent	Packet Received	Bytes Sent	Bytes Received	Source Country Code	Destination Country Code
12/22/2017 11:58:48 AM	XG310	Appliance Access	Denied	deby	contoso	172.16.100.110	255.255.255.17500	5255	17500	90:81:1c:a0:5f:5d	Social Networking	Browser Based	0	0	Information	Deny		0	0	0	0		
12/22/2017 11:58:48 AM	XG310	Appliance Access	Denied	franc	contoso	172.16.100.117	172.16.100.138	255	138	00:83:1e:93:24:88	online streaming	Network Protocol	0	0	Information	Deny		0	0	0	0		
12/22/2017 11:58:48 AM	XG310	Firewall Rule	Allowed	franc	contoso	172.16.100.142	128.177.43.65	62282	80	00:00:00:00:00:00	BITS	Infrastructure Protocol	2	0	Information	Allow		6	6	618	672	R1	USA
12/22/2017 11:58:48 AM	XG310	Firewall Rule	Allowed	samir	acme785	172.16.100.13	63.251.171.2	55697	80	00:00:00:00:00:00	HTTP	General Internet	1	0	Information	Allow		5	5	414	451	R1	USA
12/22/2017 11:58:48 AM	XG310	Invalid Traffic	Denied	gilbert	Contoso	216.163.170.635	170.166.9.242	54591	80	00:42:5a:9f:d8:19	Social Networking	Browser Based	0	0	Information	Deny	Could not associate packet to any connection	0	0	0	0		

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/22/2017 11:58:48 AM	3333	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:04:43 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:43 timezone="PST" device\_name="XG310" device\_id=S300066C313A1A0 | log\_id=010101600001 log\_type="Firewall" log\_component="Firewall Rule" log\_subtype="Allowed" status="Allow" priority=Information duration=10 fw\_rule\_id=1 policy\_type=1 user\_name="francis" user\_gp="contoso" iap=4 ips\_policy\_id=8 appfilter\_policy\_id=0 application="BITS" application\_risk=2 application\_technology="Network Protocol" application\_category="Infrastructure" in\_interface="Port1" out\_interface="" src\_mac=00:00:00:00:00:00 src\_ip=172.16.100.142 src\_country\_code=R1 dst\_ip=128.177.43.65 dst\_country\_code=USA protocol="TCP" src\_port=62282 dst\_port=80 sent\_pkts=6 sent\_bytes=818 rcv\_bytes=872 tran\_src\_ip= tran\_src\_port=0 tran\_dst\_ip=172.16.100.252 tran\_dst\_port=3128 srczone="LAN" srczone="LAN" dstzone="WAN" dstzone="WAN" dir\_disp="" connvent="Stop" connid="1730396576" vconnid="" hb\_health="No Heartbeat" message="" appressedby="Signa ture"

- Sophos Firewall - Content Filter Activity Report** - This report provides information related to all the content filtering that is done by the Sophos Firewall. Reports contains source IP, source port, username, website domain, status code, send and received bytes, category type, destination IP, destination port and other useful information to analyze in detail about the content filtering and take respective measures.

LogTime	Device Name	Component	Log Subtype	User Name	User Group	Source IP Address	Destination IP Address	Source Port	Destination Port	Category Name	Category Type	Website Domain	Url Accessed	Content Type	Priority	Status Code	Sent Bytes	Received Bytes
12/19/2017 04:32:45 PM	SG135	HTTP	Denied	atp25		15.12.19.101	172.16.6.146	49330	80	IPAddress	Acceptable	172.16.6.146	http://172.16.6.146/favicon.ico		Alert	403	0	0
12/19/2017 04:32:45 PM	SG135	HTTP	Allowed	iview1		72.16.89.15	74.125.130.188	1555	443	Search Engines	Acceptable	mtalk.google.com	http://mtalk.google.com:443/pdf	Information			0	0
12/19/2017 04:32:45 PM	CR750i NG-XP	HTTP	Allowed	bruce	Open Group	10.198.47.71	182.79.221.19	9444	443	Entertainment	Unproductive	r8---sn-c5gup-qxas.googlevideo.com	https://r8---sn-c5gup-qxas.googlevideo.com/	Information			0	319007
12/19/2017 04:32:45 PM	SG115	HTTP	Denied			192.123.59.42	216.58.197.4	46719	80	Religion & Spirituality	Unproductive	hanuman.com	http://hanuman.com/jpeg	Warning			0	0

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/19/2017 4:32:45 PM	3333	NTP/LDTBLR38 / Sophos...	N/A	N/A	Syslog

Event Type: Information  
 Log Type: Application  
 Category Id: 0

Description:  
 Dec 15 07:04:44 172.16.100.252 device="SFW" date=2017-02-01 time=18:13:29 timezone="IST" device\_name="SG135" device\_id=SFDemo1234567890 log\_id=050902616002 log\_type="Content Filtering" log\_component="HTTP" log\_subtype="Denied" status="" priority=Information fw\_rule\_id=0 user\_name="atp25" user\_gp="" iap=2 category="IPAddress" category\_type="Acceptable" url="http://172.16.6.146/favicon.ico" contenttype="" override\_token="" httpresponsecode="403" src\_ip=10.20.21.179 dst\_ip=172.16.6.146 protocol="TCP" src\_port=49330 dst\_port=80 sent\_bytes=0 recv\_bytes=0 domain=172.16.6.146

- Sophos Firewall - User Authentication Success Report** - This report provides information related to all the firewall login and logout activity. Report contains username, source IP, detailed message, authentication mechanism and other useful information to keep track of authentication activities and monitor any suspicious behavior.

LogTime	Device Name	User Name	Source IP Address	User Group	Authentication Client	Authentication Mechanism	Status	Priority	Message Details	Sent Bytes	Received Bytes
12/21/2017 04:50:09 PM	CR750i NG-XP	jsmith	10.198.47.71	Open Group	Web Client	N/A	Successful	Information	User jsmith was logged out of firewall	1233	1265
12/21/2017 04:50:09 PM	CR750i NG-XP	jsmith	10.198.47.71	Open Group	Web Client	Local	Successful	Information	User jsmith of group Open Group logged in successfully to Firewall through Local authentication mechanism from 10.198.47.71		

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 4:50:09 PM	<a href="#">3333</a>	NTPLDTLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:40 timezone="IST" device_name="CR750ING-XP" device_id=C44310050024 -P29PUA log_id=062910617703 log_type="Event" log_component="Firewall Authentication" log_subtype="Authentication" status="Successful" priority=information user_name="jsmith" usergroupname="Open Group" auth_client="Web Client" auth_mechanism="N/A" reason="" src_ip=10.198.47.71 src_mac=start_time=1485866617 sent_bytes=1233 rcv_bytes=1265 message="User jsmith was logged out of firewall" name="jsmith" timestamp=1485866620			
12/21/2017 4:50:09 PM	<a href="#">3333</a>	NTPLDTLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:38 timezone="IST" device_name="CR750ING-XP" device_id=C44310050024 -P29PUA log_id=062910617701 log_type="Event" log_component="Firewall Authentication" log_subtype="Authentication" status="Successful" priority=information user_name="jsmith" usergroupname="Open Group" auth_client="Web Client" auth_mechanism="Local" reason="" src_ip=10.198.47.71 message="User jsmith of group Open Group logged in successfully to Firewall through Local authentication mechanism from 10.198.47.71" name="jsmith" src_mac=			

- Sophos Firewall - User Authentication Failed Report** - This report provides information related to all the firewall login failures that is done. Report contains username, source IP, authentication mechanism, detailed message about the event to monitor in detail to analyze suspicious activities.

LogTime	Device Name	User Name	User Group	Source IP Address	Authentication Client	Authentication Mechanism	Status	Message Details
12/21/2017 04:50:09 PM	CR750ING-XP	jsmith	Open Group	101.15.94.73	Web Client	Local	Failed	User jsmith of group Open Group failed to login to Firewall through Local authentication mechanism from 10.198.47.71

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 4:50:09 PM	<a href="#">3333</a>	NTPLDTLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:38 timezone="IST" device_name="CR750ING-XP" device_id=C44310050024 -P29PUA log_id=062910617702 log_type="Event" log_component="Firewall Authentication" log_subtype="Authentication" status="Failed" priority=information user_name="jsmith" usergroupname="Open Group" auth_client="Web Client" auth_mechanism="Local" reason="" src_ip=10.198.47.71 message="User jsmith of group Open Group failed to login to Firewall through Local authentication mechanism from 10.198.47.71" name="jsmith" src_mac=			

- Sophos Firewall - Intrusion Detected on System Report** - This report provides information related to all the IPS attack that is detected by the Sophos Firewall. Report contains username, severity, signature ID, signature message, category type, protocol, source, and destination location information such as IP, port, country code and other important information about IP's attacks detected to analyze and take appropriate actions.

LogTime	Device Name	Log Component	Log Subtype	User Name	Source Address	Destination IP Address	Source Port	Destination Port	Protocol	Category Name	Signature ID	Signature Message	Classification	Priority	Status	Platform	System	Source Country Code	Destination Country Code
12/21/2017 11:54:28 AM	CR750ING-XP	Signatures	Drop	gilbert	203.190.12.415	10.198.47.71	80	40575	TCP	Application and Software	4151209031	Autodesk Design Review GF GlobalColorTable DataSubBlock Buffer Overflow	Unknown	Warning	Windows	Client	HKG	R1	

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 11:54:28 AM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-02-01 time=12:51:35 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024 -P29PUA log_id=020804407002 log_type="IDP" log_component="Signatures" log_subtype="Drop" status="" priority=Warning idp_policy_id=2 fw_rule_id=1 user_name="" signature_id=1151209031 signature_msg="Autodesk Design Review GIF GlobalColorTable DataSubBlock Buffer Overflow" classification="Unknown" rule_priority=3 src_ip=203.190.124.15 src_country_code=HKG dst_ip=10.198.47.71 dst_country_code=R1 protocol="TCP" src_port=80 dst_port=40575 platform="Windows" category="Application and Software" target="Client"			

- Sophos Firewall - Sandbox Activity Report** - This report provides information related to all the sandbox activities. Report contains username, source IP, file name, file type, file size, reason, log subtype and other useful information for further analysis.

LogTime	Device Name	Log Component	Log Subtype	User Name	Source IP Address	File Name	File Type	File Size	Source Address	Checksum	Reason
12/21/2017 07:09:14 PM	CR750i NG-XP	Mail	Allowed					10452			eligible
12/21/2017 07:09:14 PM	CR750i NG-XP	Mail	Denied	henry@contoso.com	10.198.47.112	1.exe	application/octet-stream	8533	henry@contoso.com	83cd339302bf5e8ed5240ca6383418089c337a81	cached malicious
12/21/2017 07:09:14 PM	CR750i NG-XP	Web	Allowed					4512			eligible
12/21/2017 07:09:14 PM	CR750i NG-XP	Web	Pending	gilbert	192.168.45.12	19.exe	application/octet-stream	95	10.198.241.50	3ce799580908df9ca0dc649aa8c2d06ab267e8c8	pending
12/21/2017 07:09:14 PM	CR750i NG-XP	Web	Denied	samara	10.198.47.112	19.exe	application/octet-stream	75314	10.198.241.50	3ce799580908df9ca0dc649aa8c2d06ab267e8c8	cloud malicious

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 7:09:14 PM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:33 timezone="PST" device_name="CR750iNG-XP" device_id=C44313350024 -P29PUA log_id=138301618041 log_type="Sandbox" log_component="Mail" log_subtype="Allowed" priority=Information user_name="" src_ip=filename="" filetype="" filesize=0 sha1sum="" source="" reason="eligible" destination="" subject=""			
12/21/2017 7:09:14 PM	<a href="#">3333</a>	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:33 timezone="PST" device_name="CR750iNG-XP" device_id=C44313350024 -P29PUA log_id=138302218042 log_type="Sandbox" log_component="Mail" log_subtype="Denied" priority=Critical user_name="gaurav1@iview.com" src_ip=10.198.47.112 filename="1.exe" filetype="application/octet-stream" filesize=153006 sha1sum="83cd339302bf5e8ed5240ca6383418089c337a81" source="gaurav1@iview.com" reason="cached malicious" destination="" subject=""			

- Sophos Firewall - Security Policy Activity Report** - This report provides information related to all the security policy events. Report contains username, log type, log component, inbound and outbound interface name, packets sent and received, source and destination location info such as, IP, port, country code, zone type and other useful information for further analysis.

LogTime	Device Name	Log Component	Log Subtype	User Name	Source IP Address	Destination IP Address	Source Port	Destination Port	Source IP Address	Destination IP Address	Application Name	Sent Bytes	Received Bytes	Packet Sent	Packet Received	Inbound Interface	Outbound Interface	Source Zone Type	Destination Zone Type	Source Country Code	Destination Country Code
12/19/2017 07:08:25 PM	SG135	Appliance Access	Denied	writz	72.15.94.52	10.20.23.255	137	137	127.12.15.74	117.25.9.11	Metamurf	0	0	0	0	eth0	eth1	internal	external		
12/19/2017 07:08:25 PM	SG135	Heartbeat	Denied	atp25	192.168.14.25	10.201.4.51	49321	53	127.1.11.23	141.26.59.14	Xenoped	0	0	0	0	eth0	eth1	internal	external		
12/19/2017 07:08:25 PM	SG135	Policy Rule	Allowed	iview1	213.45.69.1	10.201.3.102	1558	54322	159.26.14.89	10.20.22.173	FTP Base	172	52	4	2	eth0	eth1	internal	external	R1	R1
12/19/2017 07:08:25 PM	SG135	Invalid Traffic	Denied	gilbert	19.56.23.17	92.123.102.7	1300	443	132.15.47.10	78.46.15.92	lolife	0	0	0	0	eth0	eth1	internal	external		
12/19/2017 07:08:25 PM	SG135	IP Spoof	Denied	jeniffer	22.14.89.63	128.0.0.1	0	0	127.3.21.14	49.30.10.65	kramerX	0	0	0	0		eth1	internal	external		

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/19/2017 7:08:25 PM	<a href="#">3333</a>	NTPLDTLR36 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information		Description:			
Log Type: Application		Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:33 timezone="PST" device_name="SG135" device_id=5FDemo1234567890 log_id=011902605151 log_type="Security Policy" log_component="IP Spoof" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" ip=0 ips_policy_id=0 appfilter_policy_id=0 application="kramerX" application_risk=0 application_tech_nology="" application_category="" in_interface="" out_interface="eth1" src_mac= src_ip=169.254.234.5 src_country_code= dst_ip=128.0.0.1 dst_country_code= protocol="ICMP" icmp_type=0 icmp_code=0 sent_pkts=0 rcv_pkts=0 sent_bytes=0 rcv_bytes=0 tran_src_ip=127.3.21.14 tran_src_port=0 tran_dst_ip=49.30.10.65 tran_dst_port=0 srczone="internal" srczone="LAN" dstzone="external" dstzone="WAN" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat"			
Category Id: 0					

- Sophos Firewall - Spam Detected on System Report** - This report provides information related to all the spam that is detected by the Sophos Firewall. Report contains source and destination location info, send, and received bytes, spam action, priority, sender and recipient name, email subject, reason, and other information useful for further analysis.

LogTime	Device Name	Log Component	Log Subtype	User Name	Source IP Address	Destination IP Address	Source Port	Destination Port	Sender Address	Recipient Address	Email Subject	Mail Size	Spam Action	Priority	Reason	Sent Bytes	Received Bytes	Source Domain Name	Destination Domain Name	Source Country Code	Destination Country Code
12/19/2017 03:02:31 PM	CR7501 NG-XP	SMTP	Allowed	gilbert	10.198.47.71	10.198.233.6	11255	25	gilbert@view.com	gilbert@view.com	GP235	391	SANDSTORM ALLOW	Information	Mail is marked Clean by Sophos Sandstorm.	0	0	view.com		R1	R1
12/19/2017 03:02:31 PM	CR7501 NG-XP	POP3	Clean	bruce	10.198.47.71	10.198.233.6	22479	110	bruce2@view.com	bruce1@view.com	EMAIL	1208	Accept	Information		0	0	view.com	view.com	R1	R1
12/19/2017 03:02:31 PM	XG310	SMTPS	Allowed		199.167.22.5.135	172.16.100.7	49939	25	3125531-41012032 dustechnology.com	jperez@ustechnology.com	FW: Lowering employee health costs by more than 20%	52505	SANDSTORM ALLOW	Information	Mail is marked Clean by Sophos Sandstorm.	0	0	c130.criticalimpact.com		USA	R1
12/19/2017 03:02:31 PM	XG310	SMTP	Probable Spam		14.186.75.202	70.166.9.243	25367	25	Jackie_McGovern@mismilabs.com	part11520296574632858@industechology.com		0	REJECT	Warning		0	0	mismilabs.com		VNM	USA

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/19/2017 3:02:31 PM	<a href="#">3333</a>	NTPLDTBRLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:04:44 172.16.100.252 device="SFW" date=2017-12-15 time=07:04:44 timezone="PST" device_name="XG310" device_id=S300066C313A1A0 log_id=045901613013 log_type="Anti-Spam" log_component="SMTPS" log_subtype="Allowed" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="INDUS_SMTP" from_email_address="3125531-410120321-100-25906-0@c130.criticalimpactinc.com" to_email_address="jperez@industechology.com" email_subject="FW: Lowering employee health costs by more than 20%" mailid="c0068cb0-1513350283" mailsize=32505 spamaction="SANDSTORM ALLOW" reason="Mail is marked Clean by Sophos Sandstorm." src_domainname="c130.criticalimpactinc.com" dst_domainname="" src_ip=199.167.225.135 src_country_code=USA dst_ip=172.16.100.7 dst_country_code=R1 protocol="TCP" src_port=49939 dst_port=25 sent_bytes=0 rcv_bytes=0 quarantine_reason="Other"			

- Sophos Firewall - System Health Status Report** - This report provides information related to all the system health status. Reports contains system utilization, memory unit, total memory, available memory, used memory, and other system monitoring fields to get detailed view about the system health.

LogTime	Device Name	Log Component	Log Subtype	Configuration	Reports	Signature	Temp	Number of users	System Utilization	User Utilization	Idle State	Memory Unit	Total Memory	Available Memory	Used Memory
12/21/2017 03:26:56 PM	SG135	Disk	Usage	13.00%	0.00%	16.00%	0.00%								
12/22/2017 12:36:34 PM	XG310	Disk	Usage	16.00%	43.00%	2.00%	1.00%								
12/22/2017 12:36:34 PM	XG310	Live User	Usage					0							
12/22/2017 12:36:34 PM	XG310	CPU	Usage						0.27%	3.41%	96.32%				
12/22/2017 12:36:34 PM	XG310	Memory	Usage									byte	12470820864	6707908608	5762912256

### Log Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:02:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:02:33 timezone="PST" device_name="XG310" device_id=S300066C313A1A0 log_id=127826618031 log_type="System Health" log_component="Disk" log_subtype="Usage" priority=Information Configuration=16.00% Reports=43.00% Signature=2.00% Temp=1.00%			
12/22/2017 12:36:34 PM	<a href="#">3333</a>	NTPLDTBRLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0		Description: Dec 15 07:02:33 172.16.100.252 device="SFW" date=2017-12-15 time=07:02:33 timezone="PST" device_name="XG310" device_id=S300066C313A1A0 log_id=127926618031 log_type="System Health" log_component="Live User" log_subtype="Usage" priority=Information users=0			

- Sophos Firewall - Virus Detected on System Report** - This report provides information related to all the virus that is detected by the Sophos Firewall. Report contains File info such as file name, file size, file path, FTP URL, source, and destination location info such as IP, port, country code, virus name, email sender and recipient address, email subject and other important information about the virus detected.

LogTime	Device Name	Log Component	Log Subtype	Source IP Address	Destination IP Address	Source Port	Destination Port	Domain Name	User Name	Sender Address	Recipient Address	Email Subject	Mail Size	Virus Name	Priority	FTP Direct	File Name	File Size	File Path	FTP Command	Url Accessed	Quarantined File	Source Country Code	Destination Country Code
12/19/2017 02:32:08 PM	MS327-LBD	HTTP	Virus	10.198.47.71	213.211.198.62	11013	80	www.eicar.org	gilbert					EICAR-AV-Test	Critical						http://www.eicar.org/download/eicar.com		R1	DEU
12/19/2017 02:32:08 PM	CR7501-NG-XP	SMTP	Allowed	11.141.28.30	10.198.233.61	1255	25	contoso.com	fona	fona@contoso.com	jake.r@contoso.com	GP235	591	Eicar.exe	Critical								R1	FRA
12/19/2017 02:32:08 PM	SG135	FTP	Virus	78.15.49.12	172.16.6.146	57330	21	Jennifer						Troj/Cspj-A	Alert	/Swtft/10	Download	1034254655	6.zip	/Test/1034254655	RETR	SFW/quarantine/TrojCspj-A	RUS	R1

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/19/2017 2:32:08 PM	3333	NTPLDTBLR38 / Sophos...	N/A	N/A	Syslog

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:03:10 172.16.100.252 device="SFW" date=2017-01-31 time=15:35:15 timezone="UTC" device\_name="MS327-LBD" device\_id=B123469823-R6 2KYU log\_id=030906208001 log\_type="Anti-Virus" log\_component="HTTP" log\_subtype="Virus" status="" priority=Critical fw\_rule\_id=2 user\_name="gilbert" iap=1 av\_policy\_name="virus="EICAR-AV-Test" url="http://www.eicar.org/download/eicar.com" domainname="www.eicar.org" src\_ip=10.198.47.71 src\_country\_code=R1 dst\_ip=213.211.198.62 dst\_country\_code=DEU protocol="TCP" src\_port=11013 dst\_port=80 sent\_bytes=0 recv\_bytes=353

- Sophos Firewall - VPN User Logon or Logoff Success Report** - This report provides information related to all the VPN login and logout activity. Report contains username, source IP, authentication mechanism, message details and other information to keep track of VPN authentication activities.

LogTime	Device Name	Log Component	User Name	User Group	Source IP Address	Authentication Client	Authentication Mechanism	Message Details
12/21/2017 05:36:33 PM	CR7501-NG-XP	VPN Authentication	jsmith	Open Group	10.198.47.71	Web Client	N/A	User jsmith was logged out of VPN
12/21/2017 05:36:33 PM	CR7501-NG-XP	VPN Authentication	jsmith	Open Group	10.198.47.71	Web Client	Local	User jsmith of group Open Group logged in successfully to VPN through Local authentication mechanism from 10.198.47.71
12/21/2017 05:36:33 PM	CR7501-NG-XP	SSL VPN Authentication	jsmith	Open Group	10.198.47.71	Web Client	N/A	User jsmith was logged out of SSL VPN
12/21/2017 05:36:33 PM	CR7501-NG-XP	SSL VPN Authentication	jsmith	Open Group	10.198.47.71	Web Client	Local	User jsmith of group Open Group logged in successfully to SSL VPN through Local authentication mechanism from 10.198.47.71

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 5:36:33 PM	3333	NTPLDTBLR38 / Sophos...	N/A	N/A	Syslog

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:40 timezone="IST" device\_name="CR7501-NG-XP" device\_id=C44310050024 -P29PUA log\_id=06310617709 log\_type="Event" log\_component="VPN Authentication" log\_subtype="Authentication" status="Successful" priority=Information user\_name="jsmith" usergroupname="Open Group" auth\_client="Web Client" auth\_mechanism="N/A" reason="" src\_ip=10.198.47.71 src\_mac= start\_time=1485866617 sent\_bytes=1233 recv\_bytes=1265 message="User jsmith was logged out of VPN" name="jsmith" timestamp=1485866620

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:38 timezone="IST" device\_name="CR7501-NG-XP" device\_id=C44310050024 -P29PUA log\_id=063110617710 log\_type="Event" log\_component="SSL VPN Authentication" log\_subtype="Authentication" status="Successful" priority=Information user\_name="jsmith" usergroupname="Open Group" auth\_client="Web Client" auth\_mechanism="Local" reason="" src\_ip=10.198.47.71 message="User jsmith of group Open Group logged in successfully to SSL VPN through Local authentication mechanism from 10.198.47.71" name="jsmith" src\_mac=

- Sophos Firewall - VPN User Logon Failed Report** - This report provides information related to all the VPN login failures that is done. Report contains username, source IP, authentication mechanism, message details and other information for further analysis.

LogTime	Device Name	Log Component	User Name	User Group	Source IP Address	Authentication Client	Authentication Mechanism	Authentication Message Details
12/21/2017 05:36:33 PM	CR750I G-XP	VPN Authenticatio n	gabriel	Open Group	10.198.47.71	Web Client	Local	User jsmith of group Open Group failed to login to VPN through Local authentication mechanism from 10.198.47.71
12/21/2017 05:36:33 PM	CR750I G-XP	SSL VPN Authenticatio n	amanda	Open Group	10.54.124.36	Web Client	Local	User jsmith of group Open Group failed to login to SSL VPN through Local authentication mechanism from 10.54.124.36

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 5:36:33 PM	3333	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog

Event Type: Information  
Log Type: Application  
Category Id: 0

Description:  
Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:13:38 timezone="IST" device\_name="CR750I G-XP" device\_id=C44310050024 -P29PUA log\_id=063110617711 log\_type="Event" log\_component="SSL VPN Authentication" log\_subtype="Authentication" status="Failed" priority=Information user\_name="amanda" usergroupname="Open Group" auth\_client="Web Client" auth\_mechanism="Local" reason="" src\_ip=10.198.47.71 message="User jsmith of group Open Group failed to login to SSL VPN through Local authentication mechanism from 10.198.47.71" name="jsmith" src\_mac=

- Sophos Firewall - WAF Traffic Accepted or Denied Report** - This report provides information related to all the traffic that is allowed and denied by the Sophos Firewall. Report contains username, send, and received bytes, user agent, reason, referrer URL, priority, URL accessed, http method, source IP and other useful information to get the detailed information which will be helpful for further analysis.

LogTime	Device Name	Log Component	User Name	Source IP Address	Local IP Address	Server Name	HTTP Method	Url Accessed	Query String	Cookie	Content Type	Action	Sent Bytes	Received Bytes	Referer Url	HTTP Status Code	Reason	Additional Information	User Agent	
12/21/2017 02:25:04 PM	CR750I NG-XP Firewall	Web Application	gilbert	10.198.23 5.254	10.198.2 33.48	www.iv lewtest. com:898 9	GET	/	?la=en	-	text/html	Error	17071	726	510	-	403	Static URL Hardening	No signature found	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101
12/21/2017 02:25:04 PM	CR750I NG-XP Firewall	Web Application	monica	202.154.2 1.94	10.198.2 33.48	www.iv lewtest. com:898 9	GET	/	queryString=cookie=	-	text/html	Information	17071	765	510	-	302	-	-	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101
12/21/2017 02:25:04 PM	CR750I NG-XP Firewall	Web Application	jenifer	10.24.94.2 54	10.198.2 33.48	www.iv lewtest. com:898 0	GET	/download/eicarcom2.zip	queryString=cookie=	;	text/html	Warning	17072	739	715	http://www.ivie.wttest.com:8990/85-0-Download.html	403	Antivirus Test	EICARAV-Test	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0

### Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 2:25:04 PM	3333	NTPLDTBLR38 / <a href="#">Sophos...</a>	N/A	N/A	Syslog

Event Type: Information  
 Log Type: Application  
 Category Id: 0

**Description:**  
 Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:03:30 timezone="IST" device\_name="CR750iNG-XP" device\_id=C44313350024-P29PUA log\_id=075000617072 log\_type="WAF" log\_component="Web Application Firewall" priority=Warning user\_name="Jeniffer" server=www.iviewtest.com:8990 sourceip=10.24.94.254 localip=10.198.233.48 ws\_protocol="HTTP/1.1" url=/download/eicarcom2.zip querystring= cookie=; PHPSESSID=jetkd9iadd9699hr77pj4q974; \_pk\_id.1.fc3a=3a6250e215194a92.1485866024.1.1485866069.1485866024; \_pk\_ses.1.fc3a="" referer=http://www.iviewtest.com:8990/65-0-Download.html method=GET httpstatus=403 reason="Antivirus" extra="EICARAV-Test" contenttype="text/html" useragent="Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0" host=10.198.235.254 responsetime=403214 bytesent=739 bytesrcv=715 fw\_rule\_id=6

## 4.4 Dashboards

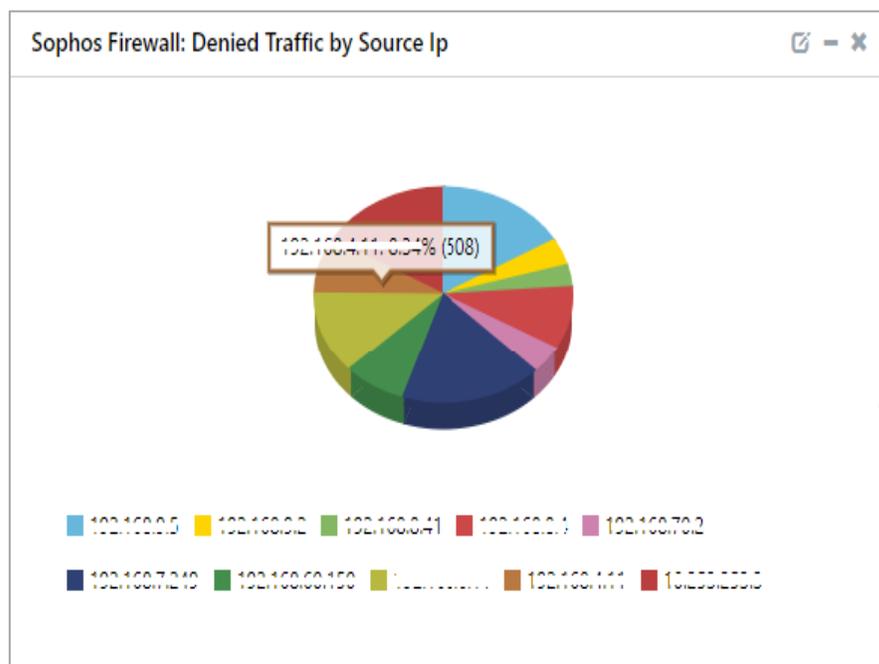
- **Sophos Firewall: VPN Activities by Geo-location**



- **Sophos Firewall: Web Traffic by Destination IP**



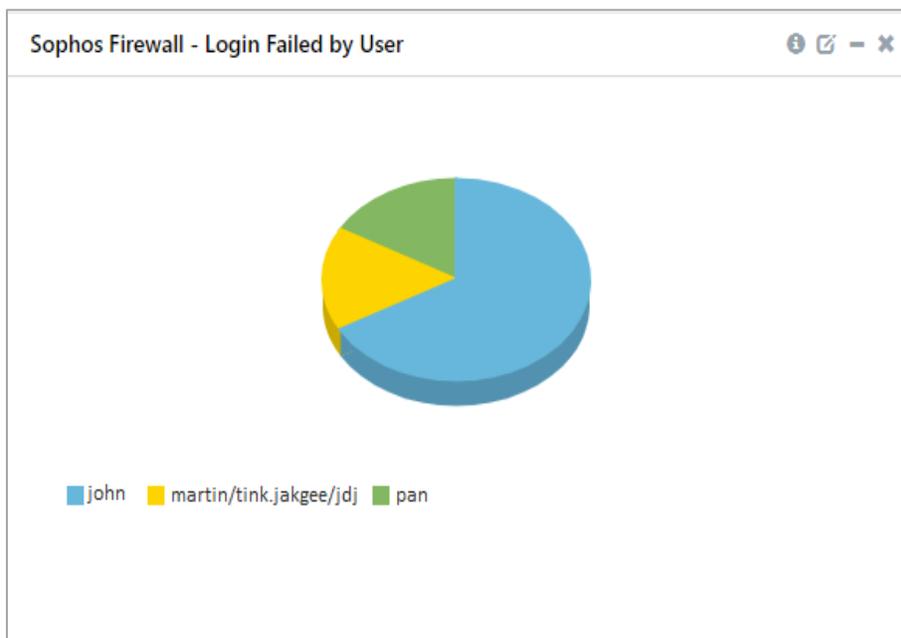
- **Sophos Firewall: Denied Traffic by Source IP**



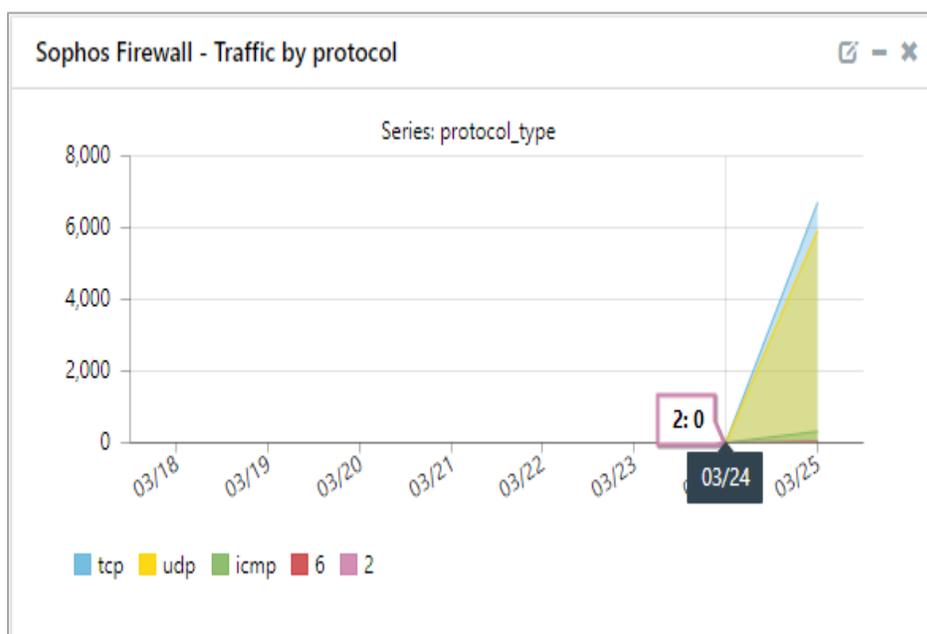
- **Sophos Firewall: Login Activities by User**



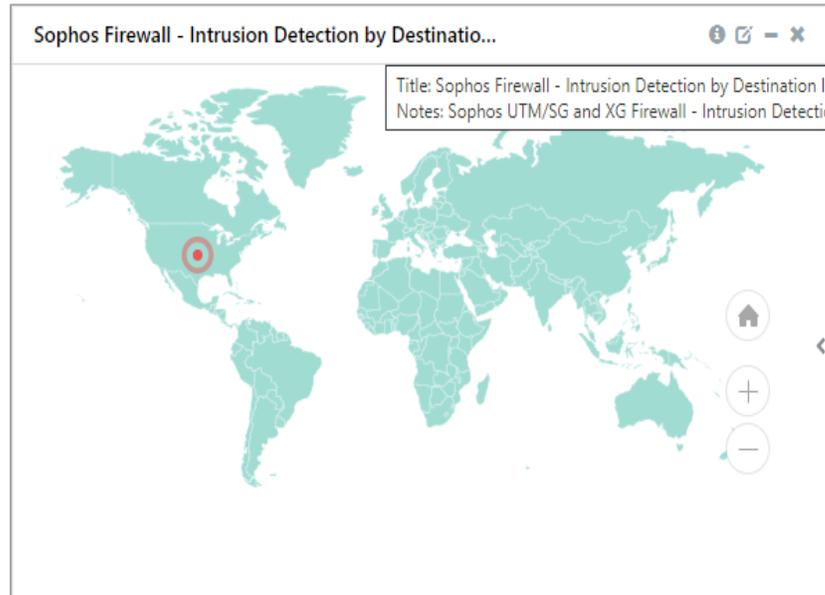
- **Sophos Firewall: Login Failed by User**



- **Sophos Firewall: Traffic by Protocol**



- **Sophos Firewall: Intrusion Detected by Destination IP geo-location**



## 5. Importing Sophos Firewall Knowledge Pack into EventTracker

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

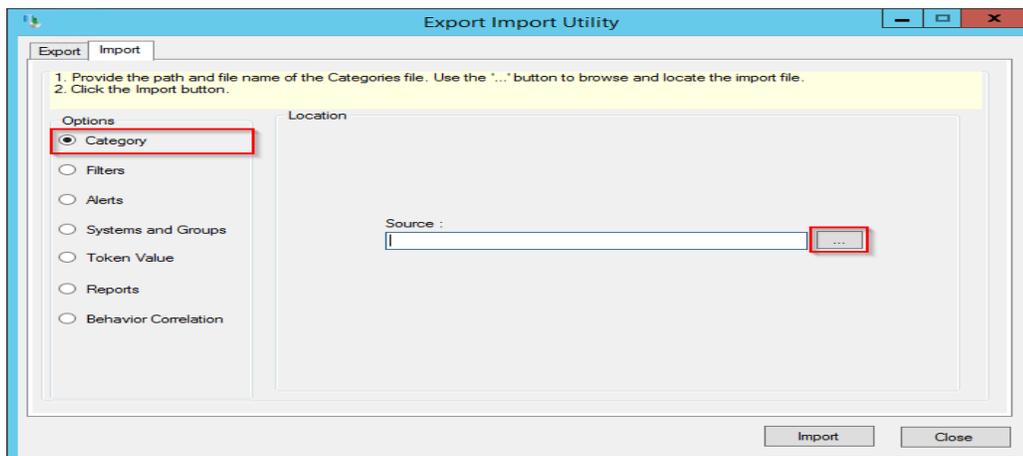
- Category
  - Token template
  - Knowledge Object
  - Report
  - Dashboard
1. Launch **EventTracker Control Panel**.
  2. Double click **Export Import Utility**.



3. Click the **Import** tab.

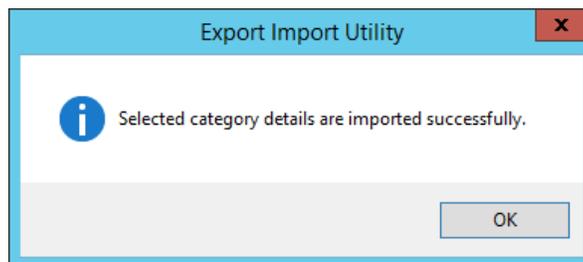
## 5.1 Category

1. Click **Category** option, and then click **Browse**  .



2. Locate **Categories\_Sophos Firewall.iscat** file, and then click **Open**.
3. To import categories, click **Import**.

EventTracker displays success message.



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

## 5.2 Token template

1. Click **Parsing rule** under **Admin** option in the EventTracker manager page.



2. Click **Template**.



- To import token template, click **Import**.



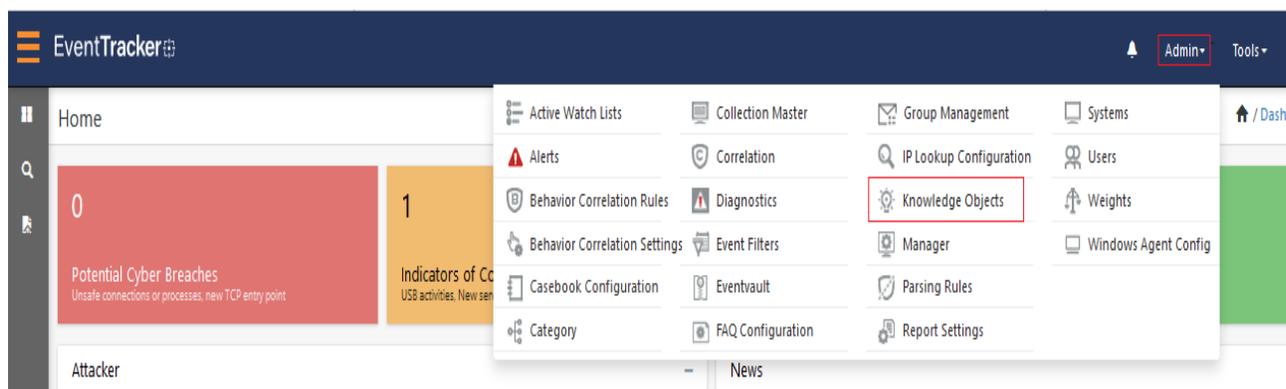
- Locate the **Templates\_Sophos Firewall.ettd** type file by clicking **Browse** button, enable all the templates, and click **import**.



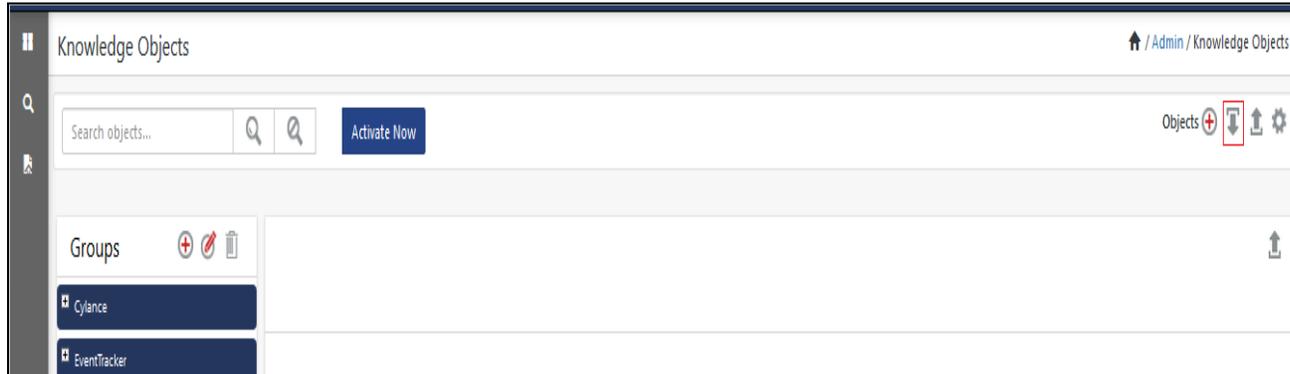
- Click **OK**.

## 5.3 Knowledge Object

- Click **Knowledge objects** under Admin option in the EventTracker manager page.



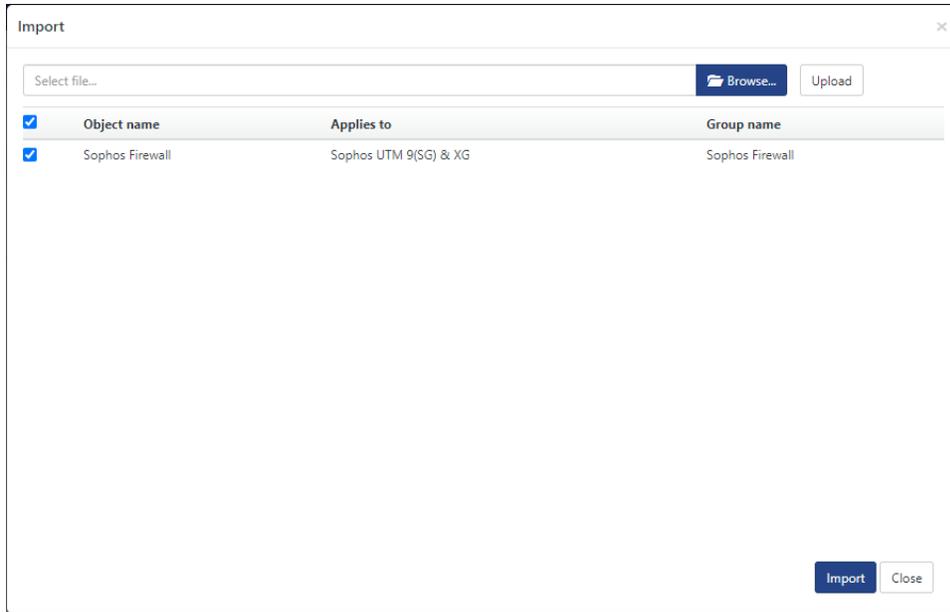
2. Click **Import**  as highlighted in the below image:



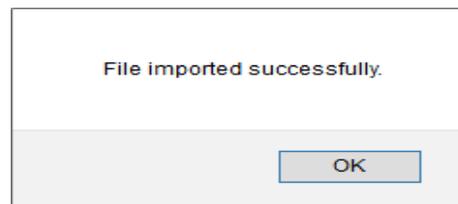
3. Click **Browse**.



4. Locate the file named **KO\_Sophos Firewall.etko**.
5. Select the check box and then click **Import** .

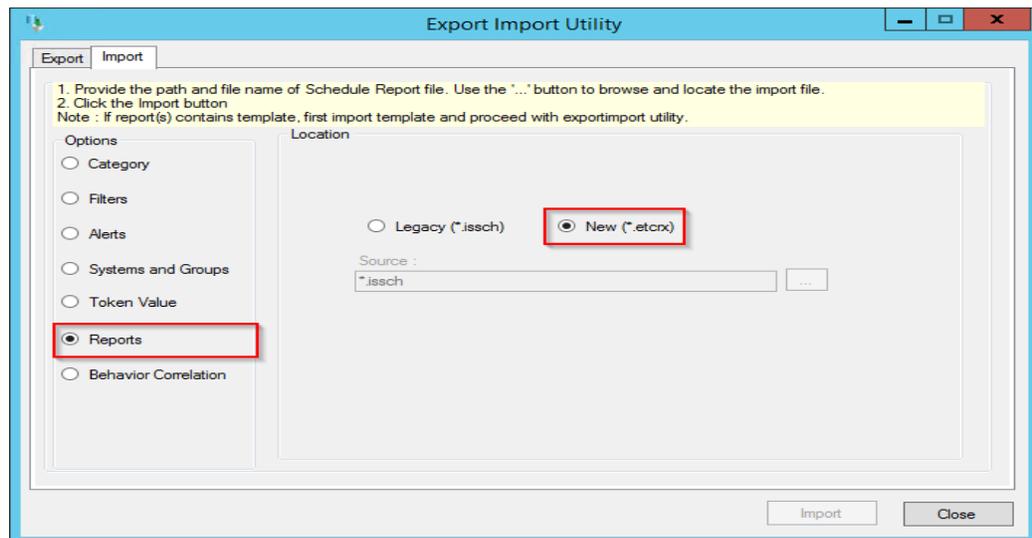


6. Knowledge objects are now imported successfully.

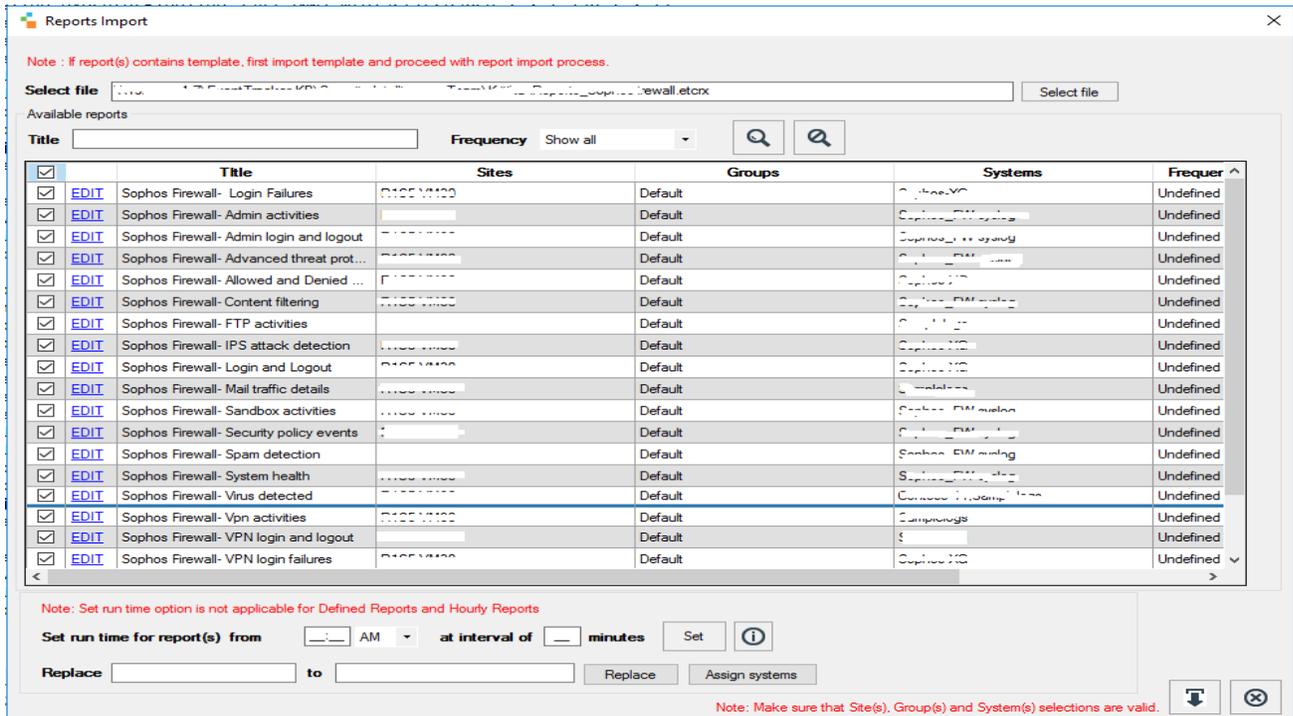


## 5.4 Report

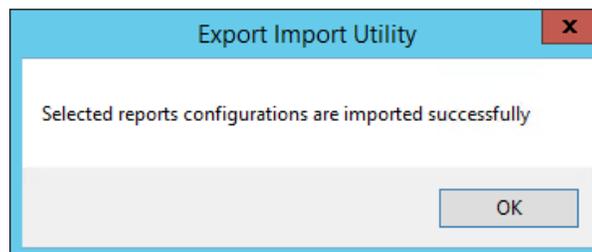
1. Click **Reports** option and select **New (\*.etcrx)** option.



2. Locate the file named **Reports\_Sophos Firewall.etcrx** and select the check box.



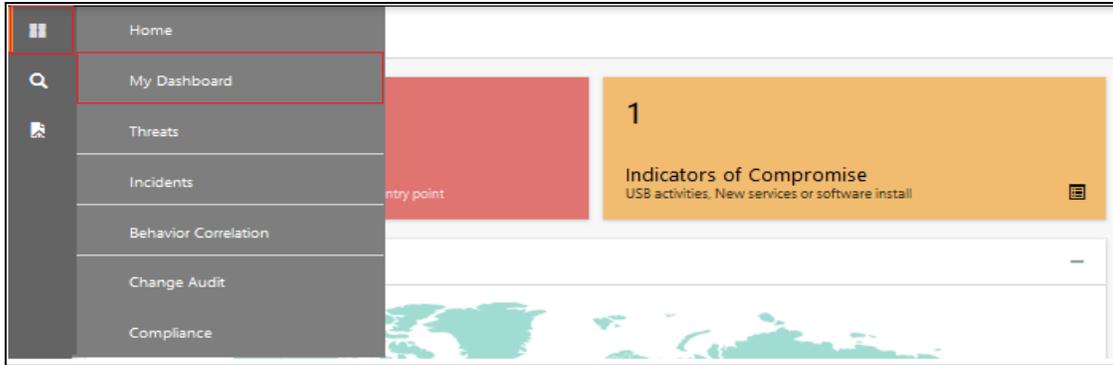
3. Click **Import** to import the report. EventTracker displays success message.



## 5.5 Dashboards

**NOTE-** Below steps given are specific to EventTracker 9.2 and later.

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



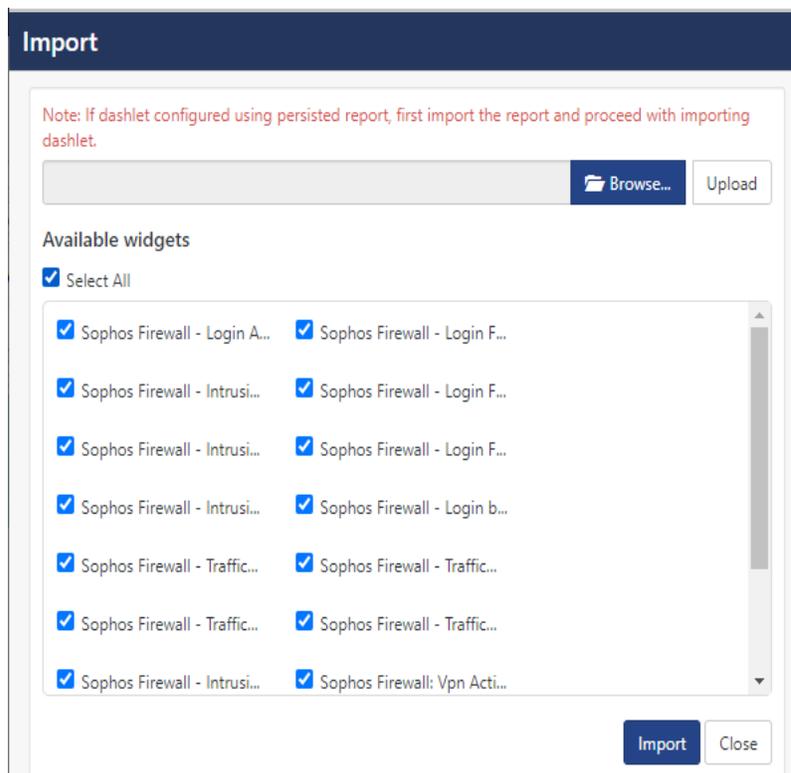
2. Navigate to **My Dashboard** option as shown above.

3. Click **Import**  as show below:

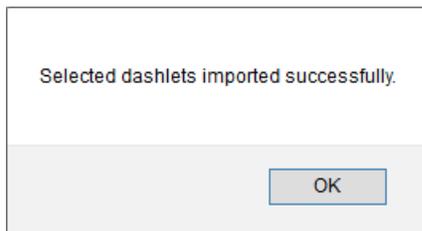


4. Import dashboard file **Dashboards\_Sophos Firewall.etwd** and select **Select All** checkbox.

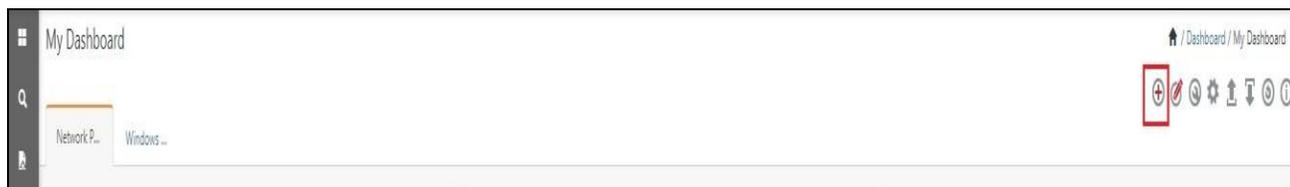
5. Click **Import** as shown below:



6. Import is now completed successfully.



7. In **My Dashboard** page select to add dashboard.



8. Choose appropriate name for **Title** and **Description**. Click **Save**.

### Add Dashboard

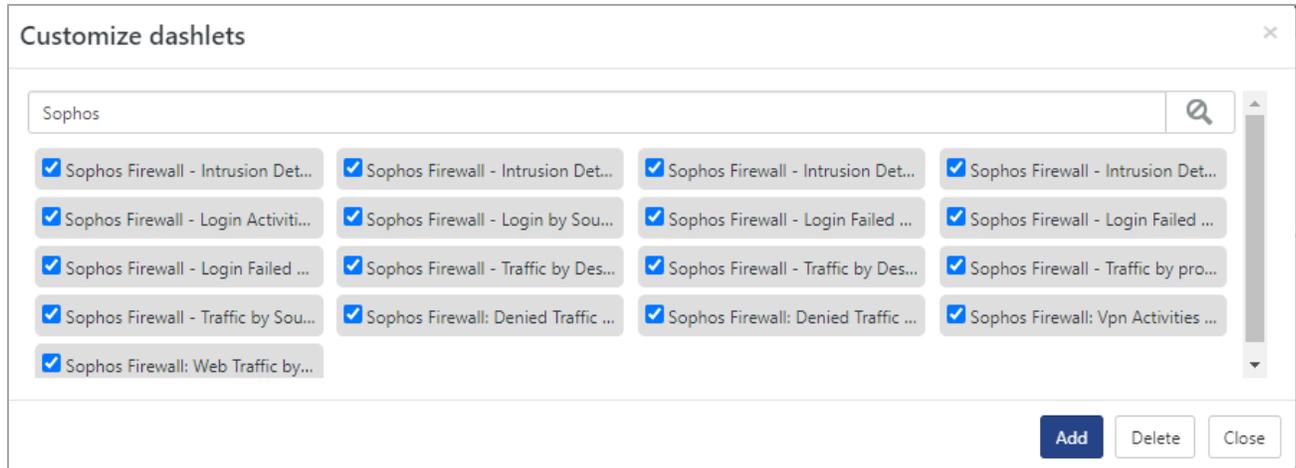
Title

Description

9. In **My Dashboard** page select to add dashlets.



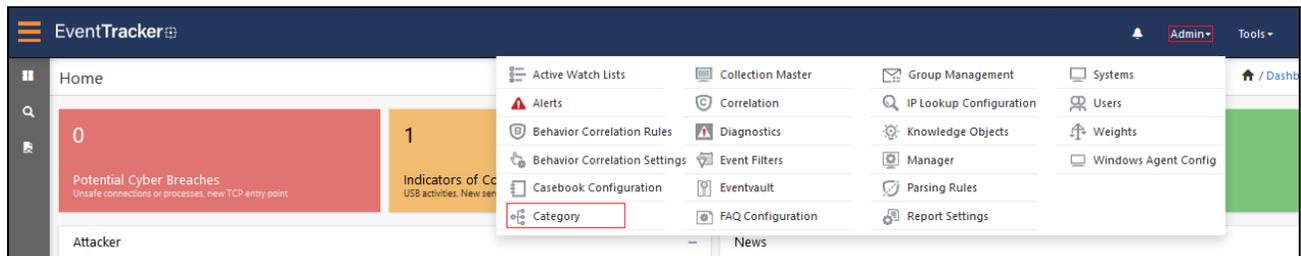
10. Select imported dashlets and click **Add**.



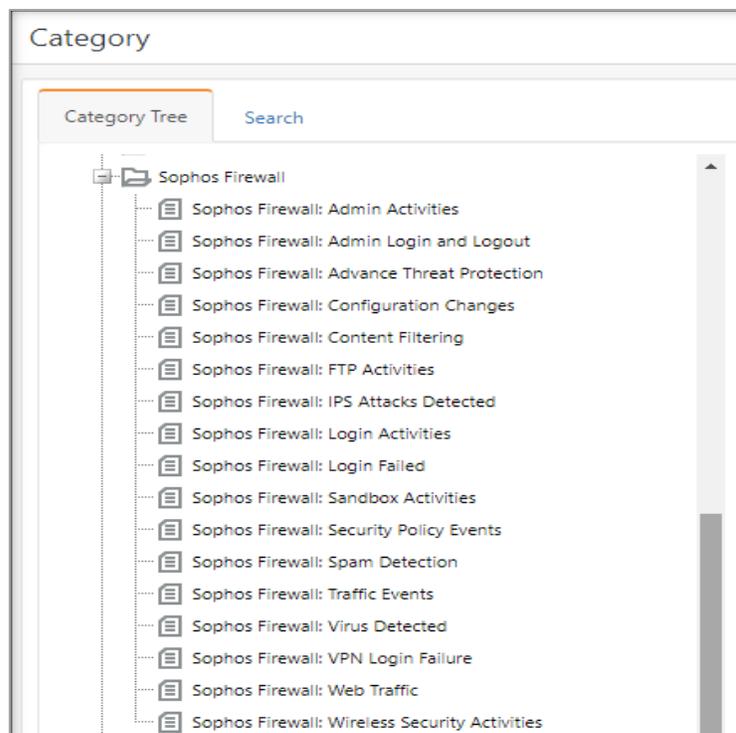
## 6. Verifying Sophos Firewall Knowledge Pack in EventTracker

### 5.6 Category

1. Logon to **EventTracker**.
2. Click **Admin** dropdown, and then click **Category**.

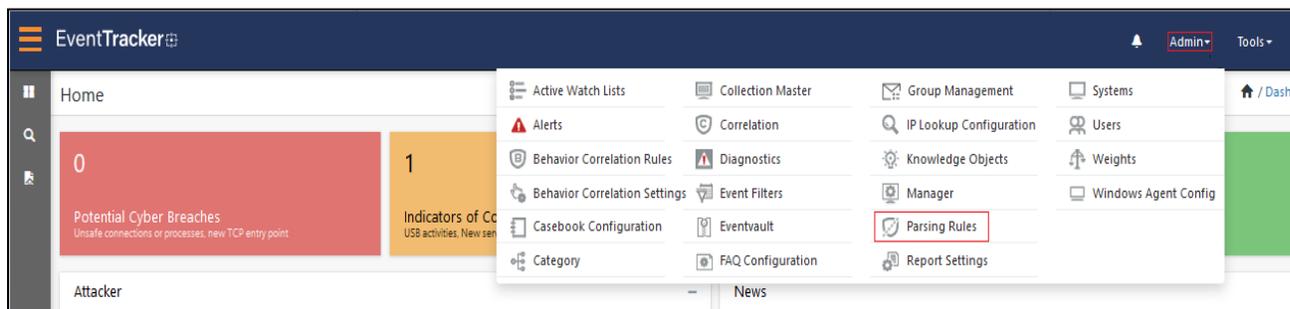


3. In **Category Tree** to view imported category, scroll down and expand **Sophos Firewall** group folder to view the imported category.

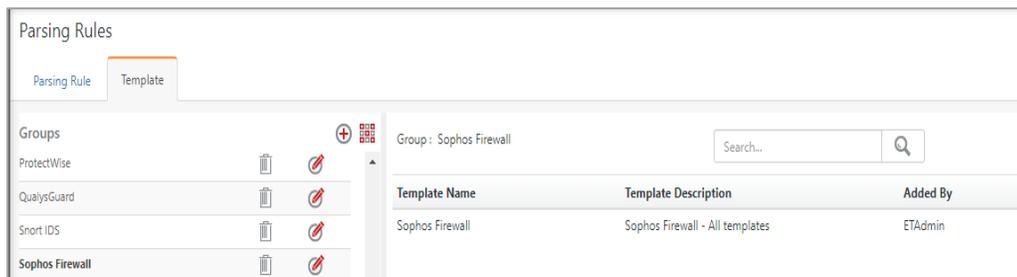


## 5.7 Token templates

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then click **Parsing rules**.

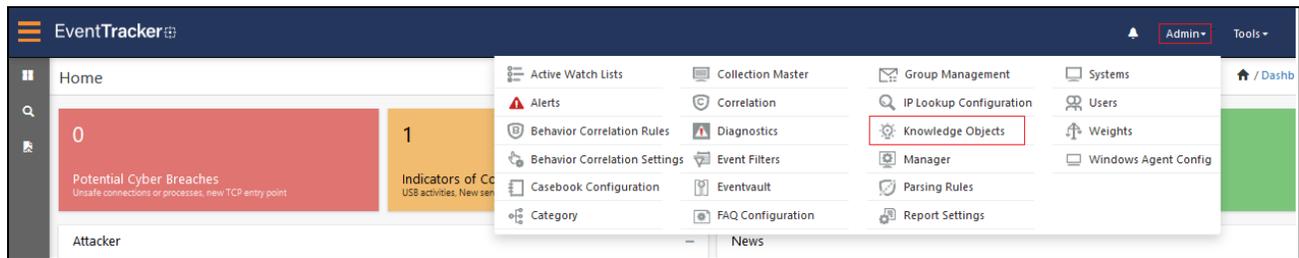


2. On **Template** tab, click on the **Sophos Firewall** group folder to view the imported token values.

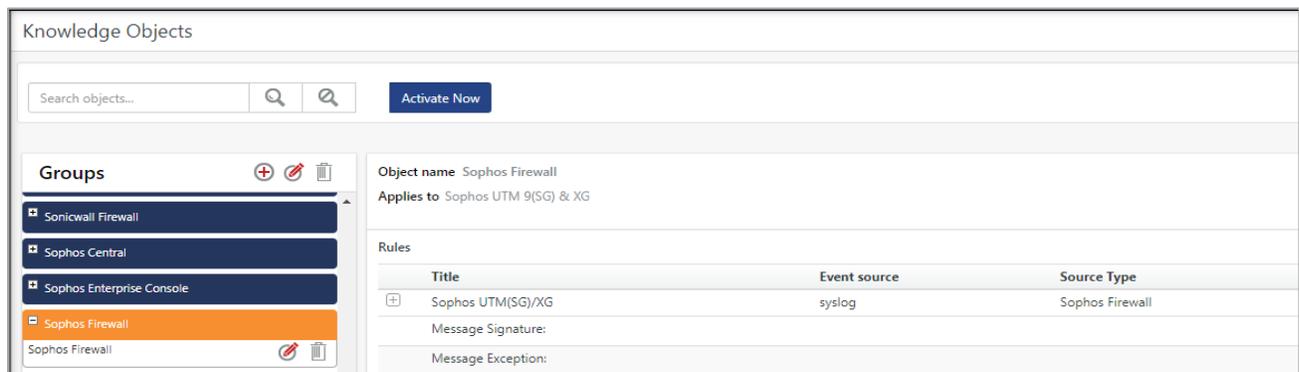


## 5.8 Knowledge Object

1. In the **EventTracker** web interface, click the **Admin** dropdown, and then select **Knowledge Objects**.



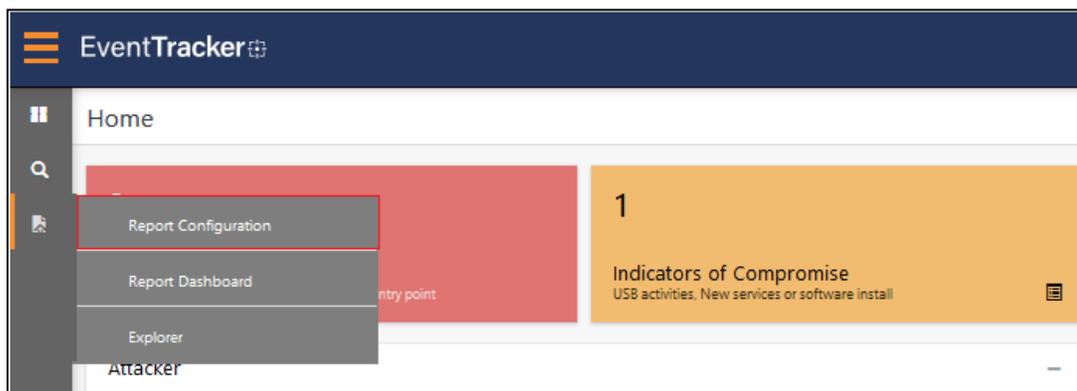
2. In the Knowledge Object tree, expand **Sophos Firewall** group folder to view the imported knowledge object.



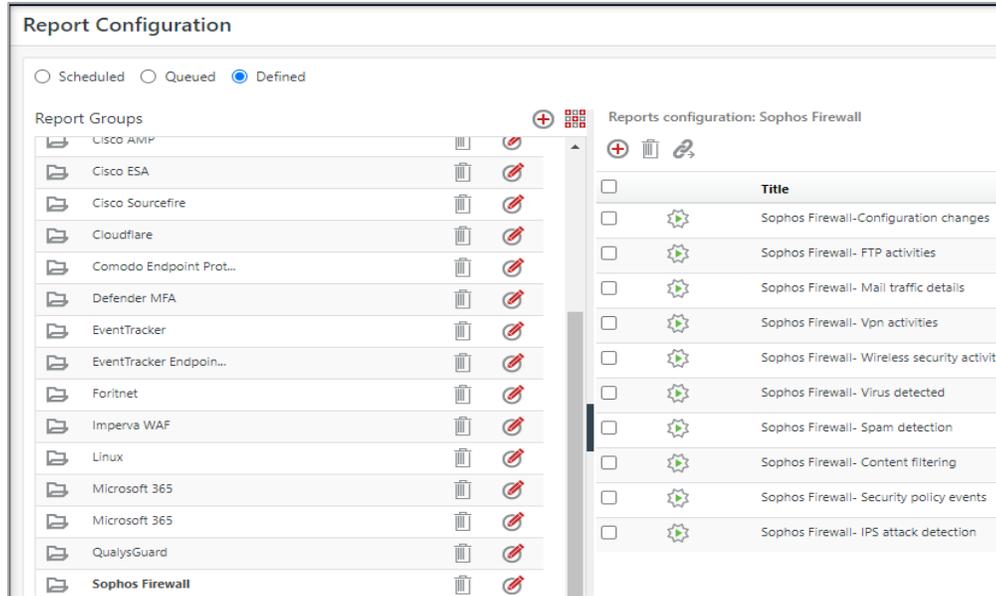
3. Click **Activate Now** to apply imported knowledge objects.

## 5.9 Report

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



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



## 5.10 Dashboards

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



2. In the **Sophos Firewall** dashboard you should be now able to view the following screen.



## About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's [EventTracker](#) cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's [BranchSDO](#) delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#). Netsurion is #19 among [MSSP Alert's 2020 Top 250 MSSPs](#).

## Contact Us

### Corporate Headquarters

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

### Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)  
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)  
EventTracker Essentials SOC: 877-333-1433 (Option 4)  
EventTracker Software Support: 877-333-1433 (Option 5)  
<https://www.netsurion.com/eventtracker-support>