

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

Та	able of Contents 3							
1	Overview 4							
2	Prerequisites 4							
3	Inte	grating 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	Evei	ntTracker Knowledge Pack	8					
	4.1	Category	8					
	4.2	Alerts	9					
	4.3	Reports	9					
	4.4	Dashboards	19					
5.	Import	ing Sophos Firewall Knowledge Pack into EventTracker	22					
	5.1	Category	23					
	5.2	Token template	23					
	5.3	Knowledge Object	24					
	5.4 Report							
	5.5	Dashboards	27					
6.	Verifyi	ng 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**.

A Local logging A Remote Sve	B Remote Log	
Cocarrogging Veniote Sys	Kennote Log	
mote syslog status		
Remote syslog settings		
Syslog Servers	+	To set up a remote syslog server, specify its location and the
🖻 🗙 logs		service il uses.
		(



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	- man

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.

Netsurion

Data Anonymization	n Traffic Shaping	Services

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		
Invalid Traffic	Image: A start and a start and a start a st	
Local ACLs		
DoS Attack		
Dropped ICMP Redirected Packet		
Dropped Source Routed Packet		
Dropped Fragmented Traffic		
MAC Filtering		
IP-MAC Pair Filtering		
IP Spoof Prevention		
SSL VPN Tunnel		
Protected Application Server		
Heartbeat		

IPS

Anomaly	
Signatures	

Anti-Virus

Netsurion_®

нттр		
FTP		
SMTP		
POP3		
IMAP		
HTTPS		
SMTPS		
POPS		
IMAPS		
Anti-Spam	_	
SMTP	✓	
POP3		
IMAP		
SMTPS		
POPS		
IMAPS	~	
Content Filtering		
Web Filter		
Application Filter	✓	
Events		
Admin Events	✓	
Authentication Events	✓	
System Events	✓	
Sandbox		
Sandstorm Event		
АТР		
ATP Events	✓	 Image: A start of the start of
Web Server Protection		

Web Server Protection Events		
------------------------------	--	--



System Health

Usage

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:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/21/2017 3:43:24 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Description: Log Type: Application Dec 15 07:04:33 172.16.100.252 device="SFW" date=2017-01-31 time=18:15:43 timezone="IST" device_name="CR750iNG-XP" device_id=C443" Category Id: 0 -P29PUA log_id=062009617502 log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" priority=Information user_imin" 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	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description Dec 15 og_id=(p=10.2)	n: 07:04:33 172.16.100.252 device="S 062009617503 log_type="Event" lo 0.20.15 message="SSL VPN Policy(i	FW" date=2017-12- g_component="GUI es) were deleted by	15 time=07:04:33 timezone="F " log_subtype="Admin" status "admin" from "10.20.20.15" us	ST" device_name="SG135" device_id=SFDemo1234567890 ="Successful" priority=Information user_name="admin" src_i ing "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	In formation	Administrator 'admin' logged out of Web Admin Console.
12/21/2017 03:43:24 PM	CR750iNG-XP	GUI	admin	10.198.47.71	Successful	In formation	Administrator 'admin' logged in via Web Admin Console.

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 3:43:24 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29P(min" si	n: ; 07:04:33 172.16.100.252 device= JA log_id=062009617507 log_typ; rc_ip=10.198.47.71 message="Adr	"SFW" date=2017-0" e="Event" log_comp ninistrator 'admin' lo	-31 time=18:15:50 ti onent="GUI" log_sub ogged in via Web Adi	imezone="IST" device_name="CR750iNG-XP" device_id=C44313350024 otype="Admin" status="Successful" priority=Information user_name="ao min 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.

Netsurion

LogTime		Device Name	Log Component	Log t Subtype	User Name	Source IP Address	Destination IP Address	Source Port	Destination Port	Url Accessed	Threat Name	Threat ID	Threat Type	Priority	Login User	Process User	Execution Path
12/21/2017 0	12:48:49 PM	SG135	Security Policy	Drop	stacy	10.15.45.110	77.91.166.16	3361	20480	77.91.166. 16	C2/Generic-A	522D2600-3A66- 4A31-A8D8- FFF8C0170F9B	Standard	Warning	ATOM10	ATAX	
12/21/2017 0	12:48:49 PM	CR750IN G-XP	Firewall	Drop	gilbert	10.198.47.71	46.161.30.47	22623	*80	46.161.30. 47:8080	C2/Generic-A	C366ACFB-7A6F- 4870-B359- A6CFDA8C85F7	Standard	Warning	DXC	Rumble994	C:\Windows\Boot\PCAT
12/21/2017 0	12:48:49 PM	SG135	HTTP Proxy	Alert	kim	198.156.34.2 1	202.31.139.173	8173	*80	http://202.3 1.139.173/	C2/Generic-A	BF9283B5- C043- 4483-8063- F890C982AD84	Standard	Warning	CYborG	UNK54	

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 2:48:49 PM	3333	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 og_id= 20480 : 9B ever	n: 07:04:33 172.16.100.252 device="S 086304418010 log_type="ATP" log sourceip=10.20.21.159 destinationi nttype="Standard" login_user="ATC	FW" date=2017-12- _component="Secur p=77.91.166.16 url= DM10" process_user:	15 time=07:04:33 timezone=" ity Policy" log_subtype="Drop 77.91.166.16 threatname=C2// ="ATAX" ep_uuid= execution_r	PST" device_name="SG135" device_id=SFDemo1234567890 " priority=Warning protocol="TCP" src_port=3361 dst_port= Seneric-A eventid=522D2600-3A66-4A31-A8D8- FFF8C0170F 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 Compon ent	Log Subtype	User Name	User Group	Source IP Address	Destinatio n IP Address	Source Port	Destination Port	Source MAC Address	Applicati on Name	Applicatio n Category	Application Technology	Applicat ion Risk	Priority Status	Message Details	Packet Sent	Packet Receive d	Sent Bytes	Recei ved Bytes	Source Country Code	Destinatio n Country Code
12/22/2017 11:58:48 AM	XG310	Appliance Access	Denied	deby	contos o	172.16.100 .110	255.255.25 5.255	17500	17500	90:b1:1c:a0: 5f:5d		Social Netwrking	Browser Based	ъ	Informati Deny on		б	б	0	0		
12/22/2017 11:58:48 AM	XG310	Appliance Access	Denied	franci s	contos o	172.16.100 .117	172.16.100 .255	138	1 38	b0:83:fe:93: 24:88		online streaming	Network Protocol	ъ	Informati Deny on		ъ	5	ъ	ъ		
12/22/2017 11:58:48 AM	XG310	Firewall Rule	Allowed	franci s	contos o	172.16.100 .142	128.177.43 .65	62282	80	00: 0:00: 0:00: 0	BITS	Infrastruct ure	Network Protocol	2	Informati Allow on		6	6	818	872	R1	USA
12/22/2017 11:58:48 AM	XG310	Firewall Rule	Allowed	samira	acme7 85	172.16.100 .13	63.251.171 .2	55697	80	00: 0:00: 0:00: 0	HTTP	General Internet	Browser Based	٩	Informati Allow on		5	5	414	451	R1	USA
12/22/2017 11:58:48 AM	XG310	Invalid Traffic	Denied	gilbert	Contos o	216.163.17 6.35	70.166.9.2 42	80	34591	00:42:5a:9f: d8:19		Social Netwrking	Browser Based	6	Informati Deny on	Could not associate packet to any connection	5	б	ъ	0		

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/22/2017 11:58:48 AM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 g_id=0 e_id=1 ion_tec 100.14 ytes=8 ="WAN ature"	in: 107:04:43 172.16.100.252 device="4 10101600001 log_type="firewall" policy_type=1 user_name="francis chnology="Network Protocol" appl 2 src_country_code=R1 dst_ip=128 18 recv_bytes=872 tran_src_ip= tra v" dstzone="WAN" dir_disp="" cor	SFW" date=2017-12- log_component="Fir s" user_gp="contoso ication_category="Ir %177:43.65 dst_count n_src_port=0 tran_d nevent="Stop" conr	15 time=07:04:43 timezone=" ewail Rule" log_subtype="Allo " lap=4 ips_policy_id=8 appfilt frastructure" in_interface="Pop y_code=USA protocol="TCP" t_ip=172.16.100.252 tran_dst id="1730396576" vconnid=""	PST" device_name="XG310" device_id=S300066C313A1A0 io wed" status="Ailow" priority=Information duration=10 fw_rul er_policy_id=0 application="BITS" application_risk=2 applicat t1" out_interface="" src_mac=00: 0:00: 000: 0 src_jp=172.16. src_port=62282 dst_port=80 sent_pkts=6 recv_pkts=6 sent_b port=3128 srczonetype="LAN" srczone="LAN" dstconetype hb_health="No Heartbeat" message="" appresolvedby="Sign

Netsurion®

• 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	Log Compon ent	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		15.12.19.1 01	172.16.6.146	49330	80	IPAddress	Acceptabl e	172.16.6. 146	http://172.1 6.6.146/fav icon.ico		Alert	403	ъ	б
12/19/2017 04:32:45 PM	SG135	HTTP	Allowed	iview1		72.16.89.1 5	74.125.130.1 88	1555	443	Search Engines	Acceptabl e	mtalk.goo gle.com	http://mtalk. google.com :443/	pdf	Informati on		ъ	ъ
12/19/2017 04:32:45 PM	CR750i NG-XP	HTTP	Allowed	bruce	Open Group	10.198.47. 71	182.79.221.1 9	9444	443	Entertainm ent	Unproducti ve	i r8sn- ci5gup- qxas.goo glevideo. com	https://r8 sn-ci5gup- qxas.googl evideo.com /		In formati on		ъ	319007
12/19/2017 04:32:45 PM	SG115	нттр	Denied			192.123.59 .42	216.58.197.4 4	46719	80	Religion & Spirituality	Unproducti ve	i hanuman. com	http://hanu man.com/	jpeg	Warning		ъ	5

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
12/19/2017 4:32:45 PM	3333	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 og_id= me="ai ="" http 172.16.	n. 07:04:44 172.16.100.252 device="S 050902616002 log_type="Content tp25" user_gp="" iap=2 category=" presponsecode="403" src_ip=10.20 6.146	FW" date=2017-02- Filtering" log_compo 'IPAddress" category 0.21.179 dst_ip=172.'	01 time=18:13:29 timezone=" onent="HTTP" log_subtype="D _type="Acceptable" url="http: 16.6.146 protocol="TCP" src_pr	ST" device_name="SG135" device_id=SFDemo1234567890 enied" status="" priority=Information fw_rule_id=0 user_na //172.16.6.146/favicon.ico" contenttype="" override_token ort=49330 dst_port=80 sent_bytes=0 recv_bytes=0 domain=

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



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
12/21/2017 4:50:09 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU nforma c= star	n: : 07:04:33 172.16.100.252 device= JA log_id=062910617703 log_typ stion user_name="jsmith" usergro t_time=1485866617 sent_bytes=	"SFW" date=2017 e="Event" log_co oupname="Open 1233 recv_bytes=	7-01-31 time=18:13:40 tir mponent="Firewall Autho Group" auth_client="Web 1265 message="User jsm	mezone="IST" device_name="CR750IN entication" log_subtype="Authenticatic b Client" auth_mechanism="N/A" reasc nith was logged out of firewall" name=	G-XP" device_id=C44310050024 on" status="Successful" priority=i on="" src_ip=10.198.47.71 src_ma "jsmith" timestamp=1485866620
12/21/2017 4:50:09 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PL nforma age="l mac=	m: : 07:04:33 172.16.100.252 device= JA log_id=062910617701 log_typ ation user_name="jsmith" usergrr Jser jsmith of group Open Group	"SFW" date=2017 e="Event" log_co pupname="Open logged in succes	7-01-31 time=18:13:38 tir mponent="Firewall Auth Group" auth_client="Wet sfully to Firewall through	mezone="IST" device_name="CR750iN entication" log_subtype="Authenticatic b Client" auth_mechanism="Local" reas Local authentication mechanism from	G-XP" device_id=C44310050024 on" status="Successful" priority=i on="" src_ip=10.198.47.71 mess 10.198.47.71" name=jsmith" src

• **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:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 4:50:09 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PI matior ="Use	in: ; 07:04:33 172.16.100.252 device="3 JA log_id=062910617702 log_type: n user_name="jsmith" usergroupna r jsmith of group Open Group failed	SFW" date=2017-01 ="Event" log_compo me="Open Group" a d to login to Firewall	-31 time=18:13:38 timezone= nent="Firewall Authentication suth_client="Web Client" auth, through Local authentication	"IST" device_name="CR750ING-XP" device_id=C44310050024 " log_subtype="Authentication" status="Failed" priority=Infor mechanism="Local" reason="" src_ip=10.198.47.71 message 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.

	Device	Log	Log	User	Source IP	Destination	Source	Destination		Category		Signature					Target	Source	Destination
LogTime	Name	Component	Subtype	Name	Address	IP Address	Port	Port	Protocol	Name	Signature ID	Message	Classification	Priority	Status P	latform	System	Country Code	Country Code
12/21/2017 11:54:28 AI	I CR750i G-XP	I Signatures	Drop	gilbert	203.190.12 4.15	10.198.47.7 1	80	40575	TCP	Application and Software	1151209031	Autodesk Design Review GIF GlobalColorTable DataSubBlock Buffer Overflow	Unknown	Warning	V	Vindows	Client	HKG	R1



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 11:54:28 AM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU d=1 us n="Unl port=4	n: 07:04:33 172.16.100.252 device="5 JA log_id=020804407002 log_type= er_name="" signature_id=1151209 known" rule_priority=3 src_ip=203. 0575 platform="Windows" categor	FW" date=2017-02- ="IDP" log_compone 031 signature_msg= 190.124.15 src_count ry="Application and	01 time=12:51:35 timezone= nt="Signatures" log_subtype= "Autodesk Design Review GIF try_code=HKG dst_ip=10.198, Software" target="Client"	IST" device_name="CR750ING-XP" device_id=C44313350024 "Drop" status="" priority=Warning idp_policy_id=2 fw_rule_i GlobalColorTable DataSubBlock Buffer Overflow" classificatio 47.71 dst_country_code=R1 protocol="TCP" src_port=80 dst_

• 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.

	Device	Log	Log	User	Source IP	File	File	File			
LogTime	Name	Component	Subtype	Name	Address	Name	Туре	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 @cont oso.co m	10.198.47. 112	1.exe	applicati on/octet- stream	8533	henry@contoso.co m	83cd339302bf 5e8ed5240ca6 383418089c33 7a81	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	applicati on/octet- stream	95	10.198.241.50	3ce799580908 df9ca0dc649a a8c2d06ab267 e8c8	pending
12/21/2017 07:09:14 PM	CR750i NG-XP	Web	Denied	samara	10.198.47. 112	19.exe	applicati on/octet- stream	75314	10.198.241.50	3ce799580908 df9ca0dc649a a8c2d06ab267 e8c8	cloud malicious

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE						
- 12/21/2017 7:09:14 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog						
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU e="" fil	n: 07:04:33 172.16.100.252 device= A log_id=138301618041 log_typ etype="" filesize=0 sha1sum="" :	"SFW" date=2017- e="Sandbox" log_c source="" reason="	l2-15 time=07:04:33 omponent="Mail" log eligible" destination=	timezone="PST" device_name="CR750iN0 g_subtype="Allowed" priority=Informatior ="" subject=""	G-XP" device_id=C44313350024 n user_name="" src_ip= filenam					
- 12/21/2017 7:09:14 PM	<u>3333</u>	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=2017-12-15 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@vivew.com" s rc_ip=10.198.47.112 filename="1.exe" filetype="application/octet-stream" filesize=153006 sha1sum="83cd339302bf5e8ed5240ca6383418089c337a81" s ource="gaurav1@vivew.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.

Netsurion

	Device	Loa	Log	User	Source IP	Destination	Source	Destination	Source Nat	Destination Nat IP	Applicati	Sent	Received	Packet	Packet	Inbound	Outbound	Source Zone	Destina tion Zone	Source Country	Destinatio n Country
LogTime	Name	Component	Subtype	Name	Address	IP Address	Port	Port	IP Address	Address	on Name	Bytes	Bytes	Sent	Received	Interface	Interface	Туре	Туре	Code	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	ъ	0	б	б	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 7	Xenoped	ъ	ъ	ъ	ъ	eth0	eth1	internal	external		
12/19/2017 07:08:25 PM	SG135	Policy Rule	Allowed	iview1	213.45.69.1 2	10.201.3.102	1558	34322	159.26.14.89	10.20.22.173	FTP Base	172	92	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 6	1300	443	132.15.47.10	78.46.15.92	lolife	5	ъ	ъ	ъ	eth0	eth1	internal	external		
12/19/2017 07:08:25 PM	SG135	IP Spoof	Denied	jeniffer	22.14.89.63	128.0.0.1	ъ	ъ	127.3.21.14	49.30.10.65	kramerX	ъ	ъ	ъ	ъ		eth1	internal	external		

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/19/2017 7:08:25 PM	3333	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 og_id= ule_id= nology code= t_ip=49 health=	n: 07:04:33 172:16.100.252 device="S 011902605151 log_type="Security I 0 policy_type=0 user_name="" usei ="" application_category="" in_inte protocol="ICMP" icmp_type=0 icm .30.10.65 tran_dst_port=0 srczonet; "No Heartbeat"	FW" date=2017-12- Policy" log_compone r_gp="" lap=0 ips_pc rface="" out_interfac p_code=0 sent_pkts+ ype="internal" srczo	IS time=07:04:33 timezone="P int="IP Spoof" log_subtype="C icy_id=0 appfilter_policy_id=i c=="eth1" src_mac= src_ip=168 =0 recv_pkts=0 sent_bytes=0 r ne="LAN" dstzonetype="exter	ST" device_name="SG135" device_id=SFDemo1234567890 i Denied" status="Deny" priority=Information duration=0 fw_r 0 application="kramerX" application_risk=0 application_tech 0.254.234.5 src_country_code= dst_ip=128.0.0.1 dst_country_ ecv_bytes=0 tran_src_ip=127.3.21.14 tran_src_port=0 tran_ds nal" dstzone="WAN" dir_disp="" connid="" vconnid="" hb_

• 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 Compo nent	Log Subtype	User Name	Source IP Address	Destination IP Address	Source Port	Destinatio n Port	Sender Address	Recipient Address	Email Subject	Mail Size	Spam Action	Priority	Reason	Sent Bytes	Received Bytes	Source Domain Name	Destinatio n Domain Name	Source Country Code	Destination Country Code
12/19/2017 03:02:31 PM	CR750i NG-XP	SMTP	Allowed	gilbert	10.198.47. 71	10.198.233.6 1	11255	25	gilbert@ivi ew.com	gilbert@ivi ew.com	GP235	391	SANDST ORM ALLOW	Informati on	Mail is marked Clean by Sophos Sandstorm.	б	б	iview.com		R1	R1
12/19/2017 03:02:31 PM	CR750i NG-XP	POP3	Clean	bruce	10.198.47. 71	10.198.233.6 1	22479	110	bruce2@i view.com	bruce1@iv iew.com	EMAIL	1208	Accept	Informati on		6	5	iview.com	iview.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 1-100- 25906- 0@c130.c riticalimpa ctinc.com	jperez@in dustechnol ogy.com	FW: Lowering employee health costs by more than 20%	32505	SANDST ORM ALLOW	Informati on	Mail is marked Clean by Sophos Sandstorm.	ō	ъ	c130.critic alimpactinc .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_Mc govern@ milsimlabs .com	part1.1520 2965.7463 2858@ind ustechnolo gy.com		5	REJECT	Warning		ъ	ъ	milsimlabs. com		VNM	USA



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/19/2017 3:02:31 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 g_id=0 av_poli echnold ="SANI p=199, tes=0 c	n: 07:04:44 172.16.100.252 device="S 45901613013 log_type="Anti-Spar cy_name="INDUS_SMTP" from_em: pgy.com" email_subject="FW: Lowe DSTORM ALLOW" reason="Mail is r 167.225.135 src_country_code=USA quarantine_reason="Other"	FW" date=2017-12- 1" log_component=" ail_address="312553 rring employee healt marked Clean by Sop A dst_ip=172.16.100;	15 time=07:04:44 timezone="F SMTPS" log_subtype="Allower 11-410120321-100-25906-0@c h costs by more than 20%" ma shos Sandstorm," src_domainn 7 dst_country_code=R1 protoc	PST" device_name="XG310" device_id=S300066C313A1A0 lo d" status="" priority=Information fw_rule_id=0 user_name="" 130.criticalimpactinc.com" to_email_address="Jperez@indust uild="c0066cb0-1513350283" mailsize=32505 spamaction ame="c130.criticalimpactinc.com" dst_domainname="" src_i ol="TCP" src_port=49939 dst_port=25 sent_bytes=0 recv_by

• 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	ldle 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	1 6.00%	43.00%	2.00%	1.00%								
12/22/2017 12:36:34 PM	XG310	Live User	Usage					б							
12/22/2017 12:36:34 PM	XG310	CPU	Usage						0.27%	5.41%	96.32 %				
12/22/2017 12:36:34 PM	XG310	Memory	Usage									byte	12470820 864	67079086 08	57629122 56

Log Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 g_id=1 0% Sig	n: 07:02:33 172.16.100.252 device= 27826618031 log_type="System l nature=2.00% Temp=1.00%	"SFW" date=2017-12 Health" log_compon	l-15 time=07:02:33 ti ent="Disk" log_subty	imezone="PST" device_name="XG310" /pe="Usage" priority=Information Conf	device_id=S300066C313A1A0 lo iguration=16.00% Reports=43.0
- 12/22/2017 12:36:34 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 g_id=1	n: 07:02:33 172.16.100.252 device= 27926618031 log_type="System	"SFW" date=2017-12 Health" log_compon	-15 time=07:02:33 ti ent="Live User" log_s	imezone="PST" device_name="XG310" subtype="Usage" priority=Information	device_id=S300066C313A1A0 Io 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.

Netsurion®

LogTime	Device Name	Log Comp onent	Log Subty pe	Source IP Address	Destination So IP Address e P	Destir irc ation ort Port	Domain Name	User Name	Sender Address	Recipient Address	Email Subject	Mail Size	Virus Name	Priority	F FTP D Url o	TP lirecti n	File Name	File Size	File Path	FTP Com mand	Url Accessed	Quaranti ned File	Source Country Code	Destination Country Code
12/19/2017 02:32:08 PM	MS327- LBD	нттр	Virus	10.198.47. 71	213.211.198. 1 10 62	13 80	www.ei car.org	gilbert					EICAR- AV-Test	Critical							http://www .eicar.org/d ownload/eic ar.com		R1	DEU
12/19/2017 02:32:08 PM	CR750i NG-XP	SMTP	Allowe d	11.141.26. 30	10.198.233.6 ⁴ 112 1	55 25	contoso. com	fiona	fiona@co ntoso.co m	jake.r@ac me.com	GP235	391	Eicar.ex ec	Critical									R1	FRA
12/19/2017 02:32:08 PM	SG135	FTP	Virus	78.15.49.1 2	172.16.6.146 573	30 21		Jennif er					Troj/Csp y-A,	Alert	/Swi D ft/10 a 3425 4655 6.zip	iownio d	10342 54655 6.zip	5	/Test/ 10342 54655 6.zip	RETR		SFW/qua rantine/Tr oj/Cspy- A,	RUS	R1

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
 12/19/2017 2:32:08 PM Event Type: Information Log Type: Application Category Id: 0 	3333 Descriptio Dec 15 2KYU I bert" is src_col	NTPLDTBLR38 / <u>Sophos</u> on: 07:03:10 172.16.100.252 device=" log_id=030906208001 log_type="/ ap=1 av_policy_name=" virus="EIC untry_code=R1 dst_ip=213.211.198	N/A SFW" date=2017-01 Anti-Virus" log_com; (AR-AV-Test" url="h1 8.62 dst_country_cod	N/A I-31 time=15:35:15 ti ponent="HTTP" log_s ttp://www.eicar.org/d de=DEU protocol="To	Syslog mezone="UTC" device_name="MS327-LBD" device_id=B123469823-R6 ubtype="Virus" status="" priority=Critical fw_rule_id=2 user_name="gil lownload/eicar.com" domainname="www.eicar.org" src_ip=10.198.47.71 CP" 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 12/21/2017 05:36:33 PM	Device Name CR750iNG- XP	Log Component VPN Authenticatio n	User Name jsmith	User Group Open Group	Source IP Address 10.198.47. 71	Authentication Client Web Client	Authentication Mechanism N/A	Message Details User jsmith was logged out of VPN
12/21/2017 05:36:33 PM	CR750iNG- XP	VPN Authenticatio n	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	CR750iNG- XP	SSL VPN Authenticatio n	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	CR750iNG- XP	SSL VPN Authenticatio n	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:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU rmatior start_tir	n: 07:04:33 172.16.100.252 device A log_id=063010617709 log_ty; n user_name="jsmith" usergroup me=1485866617 sent_bytes=12	="SFW" date=20 pe="Event" log_c pname="Open Gr 33 recv_bytes=12	17-01-31 time=18:13:40 tin omponent="VPN Authentic oup" auth_client="Web Cli 265 message="User jsmith"	nezone="IST" device_name="CR750ih cation" log_subtype="Authentication" ent" auth_mechanism="N/A" reason= was logged out of VPN" name="jsmit	NG-XP" device_id=C44310050024 ' status="Successful" priority=Info ="" src_ip=10.198.47.71 src_mac= th" timestamp=1485866620
12/21/2017 5:36:33 PM	3333	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU =Inform ssage= src_ma	n: 07:04:33 172.16.100.252 device IA log_id=063110617710 log_ty nation user_name="jsmith" user "User jsmith of group Open Gro c=	="SFW" date=201 pe="Event" log_c rgroupname="Op oup logged in suc	17-01-31 time=18:13:38 tin omponent="SSL VPN Auth en Group" auth_client="W cessfully to SSL VPN throug	nezone="IST" device_name="CR750Ih entication" log_subtype="Authentica eb Client" auth_mechanism="Local" r gh Local authentication mechanism fr	NG-XP" device_id=C44310050024 tion" status="Successful" priority eason="" src_ip=10.198.47.71 me om 10.198.47.71" name="jsmith"



• 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	Message Details
12/21/2017 05:36:33 PM	CR750iN 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	CR750iN 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:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 5:36:33 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PU rmatio ge="U	n: 07:04:33 172.16.100.252 device="! JA log_id=063110617711 log_type n user_name="amanda" usergroup ser jsmith of group Open Group fa	SFW" date=2017-01- ="Event" log_compo name="Open Group iled to login to SSL V	-31 time=18:13:38 timezone=" nent="SSL VPN Authenticatior " auth_client="Web Client" au /PN through Local authenticati	IST" device_name="CR750ING-XP" device_id=C44310050024 " log_subtype="Authentication" status="Failed" priority=Info th_mechanism="Local" reason="" src_ip=10.198.47.71 messa on 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.

Log 12/2	Time 1/2017 02:25:04 PM	Device Name CR750i NG-XP	Log Compon ent Web Application Firewall	User Name gilbert	Source IP Address 10.198.23 5.254	Local IP Addres s 10.198.2 33.48	Server Name www.iv iewtest. com:898 9	HTTP Method GET	Url Accessed / querystring =?la=en cookie=	Query String ?la=en	Cookie -	Content Type text/html	Priority Error	Action Taken 17071	Sent Bytes 726	Received Bytes 510	Referer Url	HTTP Status Code 403	Reason Static URL Hardening	Additional Information No signature found	User Agent Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/201001 01
12/2	1/2017 02:25:04 PM	CR750i NG-XP	Web Application Firewall	monica	202.154.2 1.94	10.198.2 33.48	www.iv iewtest. com:898 9	GET	/ querystring = cookie=			text/html	In formati on	17071	765	*510	-	502		-	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/201001 01 Firefox/50.0
12/2	1/2017 02:25:04 PM	CR750i NG-XP	Web Application Firewall	jeniffer	10.24.94.2 54	10.198.2 33.48	www.iv iewtest. com:899 0	GET	/download/ eicarcom2. zip querystring = cookie=		; PHPSES SID=jetk d9iadd9 69hsr77 jpj4q974 ; _pk_id.1 .fc3a=3	text/html	Warning	17072	739	715	http://w ww.ivie wtest.co m:8990/ 85-0- Downloa d.html	403	Antivirus	EICARAV- Test	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:50.0) Gecko/201001 01 Firefox/50.0



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
- 12/21/2017 2:25:04 PM	<u>3333</u>	NTPLDTBLR38 / Sophos	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Dec 15 -P29PL st.com kd9iad m:8990 indows	n: .07:04:33 172.16.100.252 device="3 JA log_id=075000617072 log_type" :8990 sourceip=10.24.94.254 localij :0696hsr77jpi40974; _pk.id.1.fc3a=)/85-0-Download.html method=GE : NT 6.1; WOW64; nr50.0) Gecko/20	SFW" date=2017-01- ="WAF" log_compon p=10.198.233.48 ws_ 3a6250e215194a92.1 ET httpstatus=403 rea 0100101 Firefox/50.0	31 time=18:03:30 timezone=" ent="Web Application Firewall protocol="HTTP/1.1" url=/dov 485666024.1.1485866069.148 ason="Antivirus" extra="EICAR " host=10.198.235.254 respon:	IST" device_name="CR750ING-XP" device_jd=C44313350024 I" priority=Warning user_name="jeniffer" server=www.iviewte wnload/eicarcom2.zip querystring= cookie="; PHPSESSID=jet 566024; _pk_ses.1.rc3a=" referer-http://www.iviewtest.co IAV-Test" contenttype="text/html" useragent="Mozilla/5.0 (W setime=403214 bytessent=739 bytesrcv=715 fw_rule_jd=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









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**.

E3	Even	tTracker Contro	l Panel	_ 🗆 🗙
			Ev	entTracker
EventVault	Diagnostics	License Manager	Export Import Utility	Append Archives
\$ 0	00	X	*	
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracker
2	£3			
Change Audit	About EventTracker			
	E-mail: s	support@Event Tra	cker.com	

3. Click the **Import** tab.



5.1 Category

1. Click Category option, and then click Browse .

	Export Import Utility
Export Import 1. Provide the path and file nar 2. Click the Import button.	ne of the Categories file. Use the '' button to browse and locate the import file.
Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation 	Location Source :
	Import Close

- 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.

		🔎 Admin v
Active Watch Lists	FAQ Tile Configuration	D Parsing Rules
Alerts	Group Management	Report Settings
Casebook Configuration	Q IP Lookup Configuration	Systems
● Category	- Q- Knowledge Objects	Q Users
A Diagnostics	Machine Learning Jobs	↓ ∰ Weights
Event Filters	🖓 Machine Learning Settings	
🔮 Eventvault	Manager	

2. Click Template.



Parsing Rule Template	
Groups	(+)

3. To import token template, click Import.



4. Locate the **Templates_Sophos Firewall.ettd** type file by clicking **Browse** button, enable all the templates, and click **import**.

mport	
Select file	🖙 Browse
Note: Please select file of	i type *.ettd (eventtracker template dashlets).

5. Click **OK**.

5.3 Knowledge Object

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

	Event Tracker ⊕					🐥 🛛 Admin•	Tools •
	Home		📇 Active Watch Lists	Collection Master	Croup Management	Systems	🕈 / Dashb
Q		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	Diagnostics	🔆 Knowledge Objects	r Weights	
*			🏷 Behavior Correlation Settings	🗟 Event Filters	Manager	Uindows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	P Eventvault	🕖 Parsing Rules		
			e [⁰ / ₀ Category	FAQ Configuration	🖉 Report Settings		
	Attacker			- News			

Netsurion®

2. Click Import \blacksquare as highlighted in the below image:

	Knowledge Ob	ojects		🕈 / Admin / Knowledge Objects
Q	Search objects	Q	Q Activate Now	Objects 🕀 頂 🏦 🌣
UK.	Groups	0 🖉 🗊		<u>1</u>
	E Cylance			
	• EventTracker			

3. Click Browse.



- 4. Locate the file named **KO_Sophos Firewall.etko**.
- 5. Select the check box and then click \blacksquare Import.

Netsurion®

Import				×
Select	file		🗁 Browse Upload	
<	Object name	Applies to	Group name	
	Sophos Firewall	Sophos UTM 9(SG) & XG	Sophos Firewall	
			Import Clo	se

6. Knowledge objects are now imported successfully.

File imported successfully.
ОК

5.4 Report

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

4	Export Import Utility	_		×
Export Import 1. Provide the path and file na 2. Click the Import button Note : if report(s) contains ten Options Category Filters Alerts Systems and Groups Token Value Reports Behavior Correlation	me of Schedule Report file. Use the '' button to browse and locate the import file. plate, first import template and proceed with exportimport utility. Location C Legacy (* issch) New (* etcrx) Source : * issch			
	Import		Close	e



2. Locate the file named **Reports_Sophos Firewall.etcrx** and select the check box.

vailat	l ble repo	rts			Select file	
itle			Frequency Show all	- Q Q		
		Title	Sites	Groups	Systems	Frequer ^
	<u>EDIT</u>	Sophos Firewall- Login Failures	Et 05 MM20	Default	°.'∽₀₽.₩℃	Undefined
	<u>EDIT</u>	Sophos Firewall- Admin activities		Default	C., i, Tita, i.g.	Undefined
\sim	EDIT	Sophos Firewall- Admin login and logout		Default	Coprios_1 ++ sysiog	Undefined
\square	EDIT	Sophos Firewall- Advanced threat prot	210514102	Default	0.1 _DW	Undefined
	EDIT	Sophos Firewall- Allowed and Denied	F	Default	nutrus in	Undefined
\triangleleft	EDIT	Sophos Firewall- Content filtering	T. 100 VIII00	Default	2-, 'DW	Undefined
2	EDIT	Sophos Firewall- FTP activities		Default	0.011 <u>2</u>	Undefined
2	EDIT	Sophos Firewall- IPS attack detection	L	Default	C.,:	Undefined
2	EDIT	Sophos Firewall- Login and Logout	DICEMBO	Default	2.,	Undefined
\square	<u>EDIT</u>	Sophos Firewall- Mail traffic details		Default	C-malal	Undefined
2	EDIT	Sophos Firewall- Sandbox activities		Default	Seekee SM avelog	Undefined
\square	EDIT	Sophos Firewall- Security policy events	:	Default	Cut _ DML y 1 _	Undefined
2	EDIT	Sophos Firewall- Spam detection		Default	Sachae ElW avalag	Undefined
2	EDIT	Sophos Firewall- System health		Default	S.,	Undefined
	EDIT	Sophos Firewall- Virus detected		Default	Control in John 1 1-20	Undefined
	EDIT	Sophos Firewall- Vpn activities	D1051000	Default	Cumpiciogs	Undefined
2	EDIT	Sophos Firewall- VPN login and logout		Default	5	Undefined
2	EDIT	Sophos Firewall- VPN login failures	D10514400	Default	Cupiluo 310	Undefined 🗸
						>

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

Export Import Utility	x
Selected reports configurations are imported successfully	
ОК	

5.5 Dashboards

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

1. Open EventTracker in browser and logon.



	Home			
ď	My Dashboard			
**	Threats		1	
	Incidents	ntry point	Indicators of Compromise USB activities, New services or software install	
	Behavior Correlation			
	Change Audit			-
	Compliance		Carton and	

- 2. Navigate to My Dashboard option as shown above.
- 3. Click **Import** as show below:

Event Tracker @	Ņ	Admin∓	Tools •	💽 ETAdmin 🔹
My Dashboard		f	/ Dashboar	d / My Dashboard
		•	Ø Q 🛱	1 🛛 🛈

- 4. Import dashboard file Dashboards_Sophos Firewall.etwd and select Select All checkbox.
- 5. Click **Import** as shown below:

Import			
Note: If dashlet configured using p dashlet.	persisted report, first import the report a	nd proceed with ir	nporting
		🗁 Browse	Upload
Available widgets			
Select All			
Sophos Firewall - Login A	Sophos Firewall - Login F		Î
Sophos Firewall - Intrusi	✓ Sophos Firewall - Login F		
Sophos Firewall - Intrusi	✓ Sophos Firewall - Login F		
Sophos Firewall - Intrusi	✓ Sophos Firewall - Login b		
Sophos Firewall - Traffic	✓ Sophos Firewall - Traffic		- 1
Sophos Firewall - Traffic	Sophos Firewall - Traffic		
Sophos Firewall - Intrusi	Sophos Firewall: Vpn Acti		•
		Import	Close

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	
Sophos Firewall	
Description	
Sophos UTM/SG and XG Firewall	
	Save Delete Cancel

9. In **My Dashboard** page select (a) to add dashlets.



10. Select imported dashlets and click Add.

Netsurion®

Customize dashlets			×
Sophos			٩ -
Sophos Firewall - Intrusion Det			
Sophos Firewall - Login Activiti	Sophos Firewall - Login by Sou	Sophos Firewall - Login Failed	Sophos Firewall - Login Failed
Sophos Firewall - Login Failed	Sophos Firewall - Traffic by Des	Sophos Firewall - Traffic by Des	Sophos Firewall - Traffic by pro
Sophos Firewall - Traffic by Sou	Sophos Firewall: Denied Traffic	Sophos Firewall: Denied Traffic	Sophos Firewall: Vpn Activities
Sophos Firewall: Web Traffic by			*
			Add Delete Close

6. Verifying Sophos Firewall Knowledge Pack in EventTracker

5.6 Category

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

≡	Event Tracker ⊕					🐥 🛛 Admin •	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a			Alerts	Correlation	Q IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	A Diagnostics	· Knowledge Objects	A Weights	
~			🗞 Behavior Correlation Settings	⊽ Event Filters	Manager	🔲 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	C Eventvault	🧭 Parsing Rules		
			oe Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Netsurion

Category
Category Tree Search
Sophos Firewall
🗐 Sophos Firewall: Admin Activities
🗐 Sophos Firewall: Admin Login and Logout
🗐 Sophos Firewall: Advance Threat Protection
🗐 Sophos Firewall: Configuration Changes
Sophos Firewall: Content Filtering
Sophos Firewall: FTP Activities
Sophos Firewall: IPS Attacks Detected
Sophos Firewall: Login Activities
🗐 Sophos Firewall: Login Failed
Sophos Firewall: Sandbox Activities
Sophos Firewall: Security Policy Events
Sophos Firewall: Spam Detection
Sophos Firewall: Traffic Events
Sophos Firewall: Virus Detected
🗐 Sophos Firewall: VPN Login Failure
Sophos Firewall: Web Traffic
Sophos Firewall: Wireless Security Activities

5.7 Token templates

E

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

≡	EventTracker @					🐥 🛛 Admin+	Tools +
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
٩		_	Alerts	Correlation	🔍 IP Lookup Configuration	🛱 Users	
	0	1	Behavior Correlation Rules	Diagnostics	· 🔆 Knowledge Objects	reights	
~			🇞 Behavior Correlation Settings	🐨 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			📲 Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Parsing Rules					
Parsing Rule Template					
Groups ProtectWise	Ü	÷ #	Group : Sophos Firewall	Search	Q
QualysGuard	Ĩ	0	Template Name	Template Description	Added By
Snort IDS	Ē	0	Sophos Firewall	Sophos Firewall - All templates	ETAdmin
Sophos Firewall	Ü	Ø			

5.8 Knowledge Object

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

≡	Event Tracker ⊕					Admin-	Tools -
	Home	🚰 Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb	
0			Alerts	Correlation	Q IP Lookup Configuration	Q Users	_
	0	1	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	The Weights	
×			🇞 Behavior Correlation Settings	Event Filters	Manager	🛄 Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	USB activities, New sen	Casebook Configuration	Eventvault	😥 Parsing Rules		
			Gategory Category Category	FAQ Configuration	Report Settings		
	Attacker			- News			

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

Knowledge Objects							
Search objects	ର୍ ଷ୍	Act	tivate Now				
Groups	🕀 🏈 🗓	Object name Sophos Firewall					
Sonicwall Firewall	Sonicwall Firewall						
Sophos Central		Rules					
E Sonhos Enternrise Console			Title	Event source	Source Type		
		\pm	Sophos UTM(SG)/XG	syslog	Sophos Firewall		
Sophos Firewall			Message Signature:				
Sophos Firewall	<u> </u>		Message Exception:				

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**.

EventTracker							
**	Home						
Q R	Report Configuration		1				
	Report Dashboard	ntry point	Indicators of Compromise USB activities, New services or software install				
	Explorer AttacKer			-			

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

Netsurion®

Re	por	t Configuration						
C) Sch	eduled 🔿 Queued 💿 Defined						
R	eport	t Groups			+ ==	Repo	rts configura	ation: Sophos Firewall
	Þ	CISCO AMIP		Ø		÷	i <i>2</i> ,	
		Cisco ESA		Ø		_		
		Cisco Sourcefire	Ē	Ø		-	M	
	D	Cloudflare	Ī	Ø		U	225	Sopnos Firewall-Configuration changes
	Þ	Comodo Endpoint Prot	1	Ø			2.23	Sophos Firewall- FTP activities
		Defender MFA		Ø			₹ € \$	Sophos Firewall- Mail traffic details
		EventTracker		0	11		× 💽 3	Sophos Firewall- Vpn activities
		EventTracker Endpoin	Ē	1			2.25	Sophos Firewall- Wireless security activiti
	Þ	Foritnet	Ĩ	Ø			£ £ 3	Sophos Firewall- Virus detected
	Þ	Imperva WAF		0			£\$\$	Sophos Firewall- Spam detection
		Linux		Ø	- 10		2 A	Sophos Firewall- Content filtering
		Microsoft 365		Ø			₹ € 3	Sophos Firewall- Security policy events
		Microsoft 365		Ø			5	Sophos Firewall- IPS attack detection
		QualysGuard	Ĩ	Ø			w	
	Þ	Sophos Firewall	Ē	Ø				

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 <u>EventTracker</u> 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 <u>BranchSDO</u> delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch location s. 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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