SOPHOS

Cybersecurity made simple.

SF syslog file guide 20.0

Syslog descriptions

This document provides extensive information on system log files and log viewer information of Sophos Firewall OS version 20.0.

Common fields' values and format

log_id consists of the following components in the following order:

log type	log component	log subtype	severity	message ID
2 digits	2 digits	2 digits	1 digit	5 digits

Severity/Priority: 0=Emergency 1=Alert 2=Critical 3=Error 4=Warning 5=Notice 6=Information 7=Debug

Status: 0="", 1="Allow", 2="Deny", 3="Allow Session", 4="Deny Session", 5="Successful", 6="Failed", 7="Established", 8="Terminated", 9="Renew", 10="Release", 11="Expire", 12="Would deny", 13="Connected", 14="Disconnected", 15="Interim"

In syslog configuration, you can configure the following under Antivirus, they have `log_type="Anti-Virus"`

In the log viewer these appear under Malware. There are several components within the firewall that log virus events.

Web Filter:

- HTTP
- HTTPS

Ftp

- FTP

Email

- IMAP
- IMAPS
- POP3
- POPS
- SMTPS

Antivirus (HTTP / HTTPS)

Antivirus (Web) Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_http_av_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Anti-Virus	
log_component	N/A	log_component	String			HTTP /HTTPS	
log_subtype	Log Subtype	log_subtype	String			Virus PUA Clean	
severity	N/A	N/A	String			Critical	
fw_rule_id	N/A	fw_rule_id	Number	int32			
user_name	Username	user	String	384			
web_policy_id	N/A	web_policy_id	Number	int16	The web policy that applies to this HTTP transaction		
malware	Detection	virus	String	256	The name of the malware identified by the scan engine. 0If the malware was detected by Sandstorm, this will say Sandstorm.		
url	N/A	url	String	1024	URL from which the malware was downloaded		
domain	N/A	domain	String	512	The FQDN part of the URL		
src_ip	Source IP	src_ip			The IP address from which the connection originated (client-side)		
src_country	N/A	src_country	String	64	Source country code of the source IP address based on GeoIP.		eg. "IND"
dst_ip	Destination IP	dst_ip			The IP address to which the connection is directed (server-side)		
dst_country	N/A	dst_country	String	64	Destination country code of the destination IP address based on GeoIP.		eg. "USA"
src_port	N/A	src_port			The port from which the connection originated (client-side)		
dst_port	N/A	dst_port			The port to which the connection is directed (server-side)		
bytes_sent	N/A	bytes_sent	Number	int32	The amount of data in bytes sent by the firewall to the destination		
bytes_received	N/A	bytes_received	Number	int32	The amount of data in bytes received		
http_user_agent	N/A	user_agent	String	256			
http_status	N/A	status_code	Number	int16			
log_id		N/A	String				eg. "010101600001"
device_name		N/A	String				eg "SFW"
device_model		N/A	String				eg "SF01V"
device_serial_id		N/A	String				eg "SFDemo-ff94e90"
message		message	String				eg "Malware 'EICAR-AV-Test' was detected and blocked in a download from www.eicar.org"

protocol		protocol	String				eg. "TCP"
src_zone_type		N/A	String				eg "LAN"
src_zone		N/A	String				eg. "LAN"
dst_zone_type		N/A	String				eg. "WAN"
dst_zone		N/A	String				eg. "WAN"
user_group		N/A	String				eg. "student"

Antivirus (Web) Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `http_av_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Anti-Virus	
log_component	N/A	log_component	String			HTTP /HTTPS	
log_subtype	Log Subtype	log_subtype	String			Virus PUA Clean	
priority	N/A	N/A	String			Critical	
fw_rule_id	N/A	fw_rule_id	Number	int32			
user_name	Username	user	String	384			
iap	N/A	web_policy_id	Number	int16	The web policy that applies to this HTTP transaction		
virus	Detection	virus	String	256	The name of the malware identified by the scan engine. 0If the malware was detected by Sandstorm, this will say Sandstorm.		
url	N/A	url	String	1024	URL from which the malware was downloaded		
domainname	N/A	domain	String	512	The FQDN part of the URL		
src_ip	Source IP	src_ip			The IP address from which the connection originated (client-side)		
src_country_code	N/A	src_country	String	64	Source country code of the source IP address based on GeoIP.		eg. "IND"
dst_ip	Destination IP	dst_ip			The IP address to which the connection is directed (server-side)		
dst_country_code	N/A	dst_country	String	64	Destination country code of the destination IP address based on GeoIP.		eg. "USA"
src_port	N/A	src_port			The port from which the connection originated (client-side)		
dst_port	N/A	dst_port			The port to which the connection is directed (server-side)		
sent_bytes	N/A	bytes_sent	Number	int32	The amount of data in bytes sent by the firewall to the destination		
recv_bytes	N/A	bytes_received	Number	int32	The amount of data in bytes received		
user_agent	N/A	user_agent	String	256			
status_code	N/A	status_code	Number	int16			
log_id		N/A	String				eg. "010101600001"
device		N/A	String				eg "SFW"
device_name		N/A	String				eg "SF01V"

device_id		N/A	String				eg "SFDemo-ff94e90"
message		message	String				eg "Malware 'EICAR-AV-Test' was detected and blocked in a download from www.eicar.org"
protocol		protocol	String				eg. "TCP"

Sample logs

Message ID	Log
8001	device="SFW" date=2016-12-02 time=18:48:18 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=034806208001 log_type="Anti-Virus" log_component="HTTPS" log_subtype="Virus" status="" priority=Critical fw_rule_id=2 user_name="rich" iap=13 av_policy_name="" virus="EICAR-AV-Test" url="https://secure.eicar.org/eicar.com" domainname="secure.eicar.org" src_ip=192.168.73.220 src_country_code=R1 dst_ip=213.211.198.58 dst_country_code=DEU protocol="TCP" src_port=51499 dst_port=443 sent_bytes=0 recv_bytes=353 device="SFW" date=2016-12-02 time=18:57:57 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=030906208001 log_type="Anti-Virus" log_component="HTTP" log_subtype="Virus" status="" priority=Critical fw_rule_id=0 user_name="rich" iap=13 av_policy_name="" virus="Sandstorm" url="http://floater.baldrys.ca/badb.exe" domainname="floater.baldrys.ca" src_ip=192.168.73.220 src_country_code=R1 dst_ip=192.168.73.220 dst_country_code=R1 protocol="TCP" src_port=54110 dst_port=80 sent_bytes=0 recv_bytes=1594715
8003	Not currently logged in syslog

Antivirus (FTP)

Antivirus (FTP) Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `ftp_av_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Max length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Anti-Virus	
log_component	N/A	log_component	String			FTP	
log_subtype	Log Subtype	log_subtype	String			Virus Clean	
priority	N/A	N/A	String				
fw_rule_id	N/A	fw_rule_id	Number	int32			
user_name	Username	user	String	384			
virus	Detection	virus	String	256	Name of detected virus		
FTP_url	N/A	url	String	1024	URL of download/upload		
FTP_direction	N/A	direction			Download/Upload	Download Upload	
filename	N/A	file_name	String	64	Downloaded/uploaded filename		
file_size	N/A	file_size	Number	32	Size of the downloaded/uploaded file		
file_path	N/A	file_path	String	1024	Path the file was uploaded /downloaded to/from		
ftpcommand	N/A	cmd	String	64	FTP command	RETR STOR	
src_ip	Source IP	src_ip			Source IP address		
src_country_code	N/A	src_country	String	64	Source country code of the source IP address		eg. "IND" "USA"
dst_ip	Destination IP	dst_ip			The destination IP address.		
dst_country_code	N/A	dst_country	String	64	Destination country code of the destination IP address		eg. "IND" "USA"
src_port	N/A	src_port					
dst_port	N/A	dst_port					
dstdomain	N/A	domain	String	512			
sent_bytes	N/A	bytes_sent	Number	int32			
recv_bytes	N/A	bytes_received	Number	int32			
log_id		N/A	String				eg. "010101600001"
device		N/A	String				eg "SFW"
device_name		N/A	String				eg "SF01V"
device_id		N/A	String				eg "SFDemo-ff94e90"
message		message	String				eg "Malware 'EICAR-AV-Test' was detected and blocked in a download from www.eicar.org"
protocol		protocol	String				eg. "TCP"

Sample logs

Message ID	Log
9001	device="SFW" date=2018-06-21 time=19:50:23 timezone="CEST" device_name="SF01V" device_id=SFDemo-2df0960 log_id=031006209001 log_type="Anti-Virus" log_component="FTP" log_subtype="Virus" priority=Critical fw_rule_id=0 user_name="" virus="EICAR-AV-Test" FTP_url="/var/www//home/ftp-user/ta_test_file_1ta-cl1-46" FTP_direction="Upload" filename="/home/ftp-user/ta_test_file_1ta-cl1-46" file_size=0 file_path="/var/www//home/ftp-user/ta_test_file_1ta-cl1-46" ftpcommand="STOR" src_ip=10.146.13.49 src_country_code=R1 dst_ip=10.8.142.181 dst_country_code=R1 protocol="TCP" src_port=39910 dst_port=21 dstdomain="" sent_bytes=0 recv_bytes=0
9002	device="SFW" date=2018-06-21 time=19:50:48 timezone="CEST" device_name="SF01V" device_id=SFDemo-2df0960 log_id=031001609002 log_type="Anti-Virus" log_component="FTP" log_subtype="Allowed" priority=Information fw_rule_id=0 user_name="" virus="" FTP_url="/var/www//home/ftp-user/ta_test_file_1ta-cl1-46" FTP_direction="Download" filename="/home/ftp-user/ta_test_file_1ta-cl1-46" file_size=19926248 file_path="/var/www//home/ftp-user/ta_test_file_1ta-cl1-46" ftpcommand="RETR" src_ip=10.146.13.49 src_country_code= dst_ip=10.8.142.181 dst_country_code= protocol="TCP" src_port=39936 dst_port=21 dstdomain="" sent_bytes=0 recv_bytes=19926248

Antivirus (FTP) Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_ftp_av_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Max length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Anti-Virus	
log_component	N/A	log_component	String			FTP	
log_subtype	Log Subtype	log_subtype	String			Virus Clean	
severity	N/A		String				
fw_rule_id	N/A	fw_rule_id	Number	int32			
user_name	Username	user	String	384			
malware	Detection	virus	String	256	Name of detected virus		
url	N/A	url	String	1024	URL of download/upload		
con_direction	N/A	direction			Download/Upload	Download Upload	
file_name	N/A	file_name	String	64	Downloaded/uploaded filename		
file_size	N/A	file_size	Number	32	Size of the downloaded/uploaded file		
file_path	N/A	file_path	String	1024	Path the file was uploaded /downloaded to/from		
ftpcommand	N/A	cmd	String	64	FTP command	RETR STOR	
src_ip	Source IP	src_ip			Source IP address		
src_country	N/A	src_country	String	64	Source country code of the source IP address		eg. "IND" "USA"
dst_ip	Destination IP	dst_ip			The destination IP address.		
dst_country	N/A	dst_country	String	64	Destination country code of the destination IP address		eg. "IND" "USA"
src_port	N/A	src_port					
dst_port	N/A	dst_port					
dstdomain	N/A	domain	String	512			
sent_bytes	N/A	bytes_sent	Number	int32			

recv_bytes	N/A	bytes_received	Number	int32			
log_id			String				eg. "010101600001"
device_name			String				eg "SFW"
device_model			String				eg "SF01V"
device_serial_id			String				eg "SFDemo-ff94e90"
message			String				eg "Malware 'EICAR-AV-Test' was detected and blocked in a download from www.eicar.org"
protocol			String				eg. "TCP"
log_version			Number			1	eg. log_version=1
src_zone_type			String				eg. src_zone_type="LAN"
src_zone			String				eg. src_zone="LAN"
dst_zone_type			String				eg. dst_zone_type="WAN"
dst_zone			String				eg. dst_zone="WAN"
user_group			String				eg. user_group="student"

Antivirus (Mail)

See section Email (antivirus)

Reporting

- Reports under
  - Web Virus: Reports > Applications & Web > Blocked Web Attempts
  - FTP Clean: Reports > Applications & Web > FTP Usage
  - FTP Virus: Reports > Applications & Web > FTP Protection
- Log identifier for reports
  - Web Virus: Log Component = (HTTP or HTTPS) & Log Subtype = Virus
  - FTP Clean: Log Component = FTP & Log Subtype = (Allowed or Clean)
  - FTP Virus: Log Component = FTP & Log Subtype = Virus

Appliance

Reporting

- CFR Reports under
  - Log Viewer & Search
- SF On Box Reports under
  - Appliance: Reports > Compliance > Events > System Events
- Log identifier for reports
  - Appliance: Log Type = Event & Log Subtype = System & Log Component = Appliance

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_appliance_log_fmt`.

Syslog field name	Data type	Length	Format/Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		2018-12-07T10:03:48+0000
device_name	String				
device_model	String				
device_serial_id	String				
log_id	String				
log_type	String			Event	
log_component	String			Appliance Guest User Appliance Access	
log_subtype	String			System	
log_version					
severity	String			Warning Information Notification	
message	String	1024			

Sample logs

Message ID	Log
17807	
17808	
17809	
17810	
17811	
17812	
17816	
17923	

17924	
17925	
17926	
17927	
17928	
17929	
17930	
17931	
17932	
17933	
17934	
17913	
17941	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `appliance_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type		log_type	String			Event	
log_component		log_component	String			Appliance Guest User Appliance Access	
log_subtype		log_subtype	String			System	
priority			String			Warning Information Notification	
message		message	String	1024			

Sample logs

Message ID	Log
17807	
17808	
17809	
17810	
17811	
17812	
17816	
17923	

17924	
17925	
17926	
17927	
17928	
17929	
17930	
17931	
17932	
17933	
17934	
17913	
17941	

Application filter

Reporting

- CFR Reports under:
  - Bandwidth usage
  - Log viewer & search
- SF on-box reports under:
  - Application denied: Reports > Application & Web > Blocked User Apps
  - Also use to report:
    - Synchronised Application (Where appresolvedby = EAC) : Reports > Application & Web > Synchronised Application
- Log identifier for reports:
  - Application denied: Log type = Content filtering & Log component = Application & Log subtype = denied

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_appflt_deny_log_fmt`.

Syslog field name	Data type	Length	Format/Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. 2018-12-07T10:03:48+0000
device_model	String				eg. XG135
device_name	String			SFW	
device_serial_id	String				eg. C44313350024-P29PUA
log_id	String				eg. 010101600001
log_type	String			Content Filtering	
log_subtype	String			Denied	
log_version	Number				eg. log_version=1
severity	String			Information	
fw_rule_id	Number	int32	Firewall rule id		e.g. fw_rule_id=1
user_name	String	384		"" or "<username>"	
user_group	String	1024		"" or "<groupname>"	
app_filter_policy_id	Number	int16	Id of application filter policy		
category	String	64	Category in which application is categorized	Categories present in IPS signature set	
app_name	String	64	Application Name	Applications present in IPS signature set	
app_risk	Number	8	Risk in which application is categorized	Risks present in IPS signature set	
app_technology	String	32	Technology in which application is categorized	Technologies present in IPS signature set	
app_category	String	64	Category in which application is categorized	Categories present in IPS signature set	
src_ip				<Src IP address>	
src_country	String	64	ISO 3166 (A 3) Code		
dst_ip				<Dst IP address>	
dst_country	String	64	ISO 3166 (A 3) Code		

src_port					
dst_port					
bytes_sent	Number	int32			
bytes_received	Number	int32			
message	String	1024			
app_is_cloud	Boolean			true false	
parent_app	String				eg. parent_app="Skype"
parent_app_category	String				eg. parent_app_category="Instant Messaging"
parent_app_risk	Number				eg. parent_app_risk=1
classification	String			"" Sanctioned Unsanctioned New Tolerated	eg. classification="Sanctioned"
app_resolved_by	String		The module that identified the application (IPS, Micro app or SAC)	Signature Proxy EAC	
qualifier	String				eg. qualifier="Mapped"
status	String			Deny	

Sample logs

Message ID	Logs
17051	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `appflt_deny_log_fmt`.

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type	log_type	String			Content Filtering	
log_component	log_component	String			Application	
log_subtype	log_subtype	String			Denied	
priority		String			Information	
fw_rule_id	fw_rule_id	Number	int32	Firewall rule id		e.g. fw_rule_id=1
user_name	user	String	384		"" or "<username>"	
user_gp	user_group	String	1024		"" or "<groupname>"	
application_filter_policy	appfilter_policy_id	Number	int16	Id of application filter policy		
category	category	String	64	Category in which application is categorized	Categories present in IPS signature set	

application_name	app_name	String	64	Application Name	Applications present in IPS signature set	
application_risk	app_risk	Number	8	Risk in which application is categorized	Risks present in IPS signature set	
application_technology	app_technology	String	32	Technology in which application is categorized	Technologies present in IPS signature set	
application_category	app_category	String	64	Category in which application is categorized	Categories present in IPS signature set	
src_ip	src_ip				<Src IP address>	
src_country_code	src_country	String	64			
dst_ip	dst_ip				<Dst IP address>	
dst_country_code	dst_country	String	64			
src_port	src_port					
dst_port	dst_port					
sent_bytes	bytes_sent	Number	int32			
recv_bytes	bytes_received	Number	int32			
status	status	String			Deny	
message	message	String	1024			
appresolvedby	appresolvedby	String		Module that identified the application (IPS, Microapp or SAC)	Signature Proxy EAC	

Sample logs

Message ID	Logs
17051	`device="SFW" date=2018-02-27 time=18:13:29 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=054402617051 log_type="Content Filtering" log_component="Application" log_subtype="Denied" priority=Information fw_rule_id=1 user_name="" user_gp="" application_filter_policy=8 category="Mobile Applications" application_name="Gtalk Android" application_risk=4 application_technology="Client Server" application_category="Mobile Applications" src_ip=5.5.5.15 src_country_code=DEU dst_ip=74.125.130.188 dst_country_code=USA protocol="TCP" src_port=49128 dst_port=5228 sent_bytes=0 recv_bytes=0 status="Deny" message="" appresolvedby="Signature"`

ATP

Reporting

- CFR Reports under
  - ATP
  - Log Viewer & Search
- SF On Box Reports under
  - ATP: Reports > Network & Threats > Advance Threat Protection
- Log identifier for reports
  - ATP: Log Type = ATP & Log Component = (Firewall or DNS or IPS or Web) & Log Subtype = (Alert or Drop)

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_atp_log_fmt`.

Syslog field name	Data type	Length	Format/Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String				eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="086320518009"
log_type	String	8	Log Type	ATP	
log_component	String	8	Log Component	Firewall DNS IPS Web	
log_subtype	String	8	Status of log	Alert Drop	
log_version	Number				eg. log_version=1
severity	String	8	severity of log	Warning Notification Information	
user_name	String	384	Appliance User Name		e.g. user_name="gaurav"
user_group	String				
src_port	Number		Source port number		
dst_port	Number		Destination port number		
src_ip	INET		Client source ip address		
dst_ip	INET		Destination IP address		
protocol	String				eg. protocol="TCP"
src_country	String				
dst_country	String				
src_zone_type	String				eg. src_zone_type="LAN"
src_zone	String				eg. src_zone="LAN"

dst_zone_type	String				eg. dst_zone_type="WAN"
dst_zone	String				
url	String	2048	Destination IP Address in string format Or Domain Or URL		
malware	String	128	Threat Name		eg. malware=C2/Generic-A
event_id	String	64	Event id		eg. event_id=C7E26E6F-0097-4EA2-89DE-C31C40636CB2
event_type	String		Event Type	Standard Extended	
reported_user	String	256	Logged user of Host		
proc_user	String	256	Host process user		
reported_id	String	40	Endpoint ID		
file_path	String	16384	Execution path		
Threatfeed	String	64	Threat feed name	“MDR threat feeds” "SophosLabs ML threat feeds“	eg. threatfeed="MDR threat feeds"

Sample logs

Message ID	Log
18009	Oct 18 04:46:59 172.16.131.1 device_name="SFW" timestamp="2023-10-18T04:46:59-0400" device_model="SF01V" device_serial_id="SFDemo-c07-gl-vm-01" log_id=086320518009 log_type="ATP" log_component="Firewall" log_subtype="Alert" log_version=1 severity="Notice" protocol="ICMP" src_ip="172.16.131.3" dst_ip="100.0.80.3" url="100.0.80.3" malware="C2/MDR-A" threatfeed="MDR threat feeds" event_id="09B9517E-AE79-48C1-89CE-ABA7D799113B" event_type="Standard" src_country="R1" dst_country="USA"
18010	Oct 18 04:49:30 172.16.131.1 device_name="SFW" timestamp="2023-10-18T04:49:30-0400" device_model="SF01V" device_serial_id="SFDemo-c07-gl-vm-01" log_id=086304418010 log_type="ATP" log_component="Firewall" log_subtype="Drop" log_version=1 severity="Warning" protocol="ICMP" src_ip="172.16.131.3" dst_ip="100.0.80.3" url="100.0.80.3" malware="C2/MDR-A" threatfeed="MDR threat feeds" event_id="FF2E604F-D94C-4713-A7C6-8ACB65CEE293" event_type="Standard" src_country="R1" dst_country="USA"

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `atp_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type		log_type	String	8	Log Type	ATP	
log_component		log_component	String	8	Log Component	Firewall DNS IPS Web	
log_subtype		log_subtype	String	8	Status of log	Alert Drop	
priority			String	8	Priority of log	Warning Notification Information	

user_name		user	String	384	Appliance User Name		e.g. user_name="gaurav"
src_port	Source Port	src_port	Number		Source port number		
dst_port	Destination Port	dst_port	Number		Destination port number		
sourceip	Source IP	src_ip	ipaddr_t		Client source ip address		
destinationip	Destination IP	dst_ip	ipaddr_t		Destination IP address		
url		url	String	2048	Destination IP Address in string format Or Domain Or URL		
threatname		threat	String	128	Threat Name		eg. threatname=C2/Generic-A
eventid		event_id	String	64	Event id		eg. eventid=C7E26E6F-0097-4EA2-89DE-C31C40636CB2
eventtype		type	String		Event Type	Standard Extended	
login_user		host_login_user	String	256	Logged user of Host		
process_user		host_process_user	String	256	Host process user		
ep_uuid		endpoint_id	String	40	Endpoint ID		
execution_path		execution_path	String	16384	Execution path		
Threatfeed	threatfeed	threatfeed	String	64	Threatfeed Name	"MDR threat feeds"/ "SophosLabs ML threat feeds"	eg. threatfeed="MDR threat feeds"

Sample logs

Message ID	Log
18009	`device="SFW" date=2018-06-05 time=08:49:00 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=086320518009 log_type="ATP" log_component="Firewall" log_subtype="Alert" priority=Notice user_name="" protocol="ICMP" src_port=0 dst_port=0 sourceip=10.198.32.89 destinationip=82.211.30.202 url=82.211.30.202 threatname=C2/Generic-A threatfeed="MDR threat feeds" eventid=C7E26E6F-0097-4EA2-89DE-C31C40636CB2 eventtype="Standard" login_user="" process_user="" ep_uuid= execution_path=""`
18010	`device="SFW" date=2017-01-31 time=18:44:31 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=086304418010 log_type="ATP" log_component="Firewall" log_subtype="Drop" priority=Warning user_name="gaurav" protocol="TCP" src_port=22623 dst_port=80 sourceip=10.198.47.71 destinationip=46.161.30.47 url=46.161.30.47 threatname=C2/Generic-A threatfeed="MDR threat feeds" eventid=C366ACFB-7A6F-4870-B359-A6CFDA8C85F7 eventtype="Standard" login_user="" process_user="" ep_uuid= execution_path=""`

Authentication (access gateway)

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - Access Gateway: Reports > Applications & Web > User Data Transfer Report
  - Also use to report:
    - Reports > Compliance > Events > Authentication Events
- Log identifier for reports:
  - Access Gateway: Log Type = Event & Log Subtype = Authentication & Log Component = Firewall Authentication

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_internet_usage_log_fmt`.

Syslog field name	Data type	Max length	Format/Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String				eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="010101600001"
log_type	String			Event	
log_component	String			Firewall Authentication	
log_subtype	String			Authentication	
log_version	Number				eg. log_version=1
severity	String			Information	
status	String				eg. status="Successful"
user_name	String	384			"JohnDoe"
user_group	String	1024			"Sales"
client_used	String	32		refer to Authentication (Events)	
auth_mechanism	String	128		"N/A"	
reason	String	128		""	
src_ip					"2.2.2.2"
src_mac	String	32			"44:85:00:81:8a:8f"
src_country	String		ISO 3166 (A 3) Code		eg. src_country="IND"
src_port	Number				eg. src_port=59859
protocol	String				eg. protocol="TCP"
dst_ip	INET		IPv4,IPv6		eg. dst_ip="20.20.20.20"
dst_country	String		ISO 3166 (A 3) Code		eg. dst_country="USA"
dst_port	Number				eg. dst_port=53
start	Timestamp		ISO 8601		eg. start="2018-12-07T10:03:48+0000"
end	Timestamp		ISO 8601		eg. end="2018-12-07T10:03:50+0000"

bytes_sent	Number	64			see below
bytes_received	Number	64			see below
message	String	1024			"User JohnDoe was logged out of firewall"
user_full_name	String	384			"Butter vom Brot"

Sample logs

Message ID	Log
17703	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is *internet_usage_log_fmt*.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Max length	Format /Description	Possible values	Notes/Examples
log_type		log_type	String			Event	
log_component		log_component	String			Firewall Authentication	
log_subtype		log_subtype	String			Authentication	
priority			String			Information	
user_name		user	String	384			"JohnDoe"
usergroupname		user_group	String	1024			"Sales"
auth_client		client_used	String	32		refer to Authentication (Events)	
auth_mechanism		auth_mechanism	String	128		"N/A"	
reason		reason	String	128		""	
src_ip		src_ip					"2.2.2.2"
src_mac		src_mac	String	32			"44:85:00:81:8a:8f"
start_time		start_time					see below
sent_bytes		bytes_sent	Number	64			see below
recv_bytes		bytes_received	Number	64			see below
message		message	String	1024			"User JohnDoe was logged out of firewall"
name		name	String	384			"Butter vom Brot"
timestamp		event_timestamp					see below

Sample logs

Message ID	Log
17703	`device="SFW" date=2017-01-31 time=18:13:40 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062910617703 log_type="Event" log_component="Firewall Authentication" log_subtype="Authentication" status="Successful" priority=Information user_name="gaurav" 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 gaurav was logged out of firewall" name="gaurav" timestamp=1485866620`

Authentication (events)

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - Web Virus: Reports > Compliance > Events
- Log identifier for reports:
  - Web Virus: Log Type = Event & Log Subtype = Authentication

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is CR_*auth_log_fmt*.

Syslog field name	Data type	Max length	Format /Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String				eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="010101600001"
log_type	String			Event	Event
log_component	String			Firewall Authentication My Account Authentication Dial-In Authentication VPN Authentication SSL VPN Authentication GUI Web Application Firewall CTA Appliance External Authentication VPN Portal Authentication	Firewall Authentication
log_subtype	String			Authentication Admin System	Authentication
log_version	Number				eg. log_version=1
severity	String			Information Notice	Information
status	String				eg. status="Successful"
user_name	String	384			"JohnDoe"
user_group	String	1024			"Sales"

client_used	String	32		"" Authentication Agent Web Client SSO Clientless L2TP IPSec PPTP CTA MyAccount Thin Client Admin Client SSLVPN NTLM Client 24online Android Client iOS Client iOS Web Client SSLVPN Portal Android Web Client Radius SSO API Client WiFi SSO API iOS Client API Android Client WAF eDirectory SSO Heartbeat	
auth_mechanism	String	128		Local "" LDAP AD RADIUS TACACS+ EDIR Azure AD SSO	

reason	String	128		Login failed wrong credentials access not allowed IP restriction MAC restriction max login limit reached multiple login not allowed Already login as clientless user Maximum allowed users limit reached LDAP account expired Clientless user is not required to login user validity expired ip lease failed no remote access VPN policy no access rights	
src_ip					1.1.1.1
src_country	String	ISO 3166 (A 3) Code			eg. src_country="IND"
message	String	1024			"Clientless user Nyarlathotep from 1.1.1.1 failed to log in to Firewall"
user_full_name	String	384			"Nyarlathotep S. exited"
src_mac	String	32			"44:85:00:81:8a:8f

Sample logs

Message ID	Log
17701	
17702	
17704	
17705	
17706	
17707	
17708	
17709	
17710	
17711	
17712	
17713	
17714	
17715	
17945	

17946	
17947	
17968	
17718	`client_used="N/A" auth_mechanism="Local" status="Successful" user_name="priya" log_type="Event" log_id="069010617718" log_subtype="Authentication" src_country="Reserved" src_ip="10.166.71.1" severity="Information" log_component="VPN Portal Authentication" message="User priya logged in successfully to VPN portal through Local authentication mechanism" bytes="0"`
17719	`reason="wrong credentials" client_used="N/A" auth_mechanism="Local" status="Failed" user_name="priya" log_type="Event" log_id="069010517719" log_subtype="Authentication" src_country="Reserved" src_ip="10.166.71.1" severity="Notice" log_component="VPN Portal Authentication" message="User priya failed to login to VPN portal through Local authentication mechanism because of wrong credentials" bytes="0"`
17720	`client_used="N/A" auth_mechanism="N/A" status="Successful" user_name="priya" log_type="Event" log_id="069010617720" log_subtype="Authentication" src_country="Reserved" src_ip="10.166.71.1" severity="Information" log_component="VPN Portal Authentication" message="User priya logged out of VPN portal" bytes="0"`

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is *auth_log_fmt*.

Syslog field name	Log viewer - Detail view field name	Data type	Max length	Format /Description	Possible values	Notes/Examples
log_type	log_type	String			Event	Event

log_component	log_component	String			Firewall Authentication My Account Authentication Dial-In Authentication VPN Authentication SSL VPN Authentication GUI Web Application Firewall CTA Appliance External Authentication VPN Portal Authentication	Firewall Authentication
log_subtype	log_subtype	String			Authentication Admin System	Authentication
priority		String			Information Notice	Information
user_name	user	String	384			"JohnDoe"
usergroupname	user_group	String	1024			"Sales"

auth_client	client_used	String	32		"" Authentication Agent Web Client SSO Clientless L2TP IPSec PPTP CTA MyAccount Thin Client Admin Client SSLVPN NTLM Client 24online Android Client iOS Client iOS Web Client SSLVPN Portal Android Web Client Radius SSO API Client WiFi SSO API iOS Client API Android Client WAF eDirectory SSO Heartbeat	
auth_mechanism	auth_mechanism	String	128		Local "" LDAP AD RADIUS TACACS+ EDIR	

reason	reason	String	128		Login failed wrong credentials access not allowed IP restriction MAC restriction max login limit reached multiple login not allowed Already login as clientless user Maximum allowed users limit reached LDAP account expired Clientless user is not required to login user validity expired ip lease failed no remote access VPN policy no access rights	
src_ip	src_ip					1.1.1.1
message	message	String	1024			"Clientless user Nyarlathotep from 1.1.1.1 failed to log in to Firewall"
name	name	String	384			"Nyarlathotep S. exited"
src_mac	src_mac	String	32			"44:85:00:81:8a:8f

Sample logs

Message ID	Log
17701	`device="SFW" date=2017-01-31 time=18:13:38 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062910617701 log_type="Event" log_component="Firewall Authentication" log_subtype="Authentication" status="Successful" priority=Information user_name="gaurav" usergroupname="Open Group" auth_client="Web Client" auth_mechanism="Local" reason="" src_ip=10.198.47.71 message="User gaurav of group Open Group logged in successfully to Firewall through Local authentication mechanism from 10.198.47.71" name="gaurav" src_mac=`
17702	
17704	
17705	
17706	
17707	`device="SFW" date=2017-03-15 time=14:33:37 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=063010617707 log_type="Event" log_component="VPN Authentication" log_subtype="Authentication" status="Successful" priority=Information user_name="gaurav" usergroupname="" auth_client="N/A" auth_mechanism="Local" reason="" src_ip=10.198.233.49 message="User gaurav logged in successfully to L2TP through Local authentication mechanism" name="" src_mac=`
17708	
17709	

17710	device="SFW" date=2017-03-15 time=17:23:00 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=063110617710 log_type="Event" log_component="SSL VPN Authentication" log_subtype="Authentication" status="Successful" priority=Information user_name="gaurav" usergroupname="" auth_client="N/A" auth_mechanism="Local" reason="" src_ip=10.198.233.49 message="User gaurav authenticated successfully to login to SSLVPN through Local authentication mechanism" name="" src_mac=
17711	
17712	
17713	
17714	
17715	
17945	
17946	
17947	
17968	
17718	messageid="17718" log_type="Event" log_component="VPN Portal Authentication" log_subtype="Authentication" status="Successful" user="priyanka" user_group="" client_used="N/A" auth_mechanism="Local" reason="" src_ip="10.171.4.169" message="User priyanka logged in successfully to VPN portal through Local authentication mechanism" name="" src_mac=""
17719	messageid="17719" log_type="Event" log_component="VPN Portal Authentication" log_subtype="Authentication" status="Failed" user="priyanka" user_group="" client_used="N/A" auth_mechanism="Local" reason="wrong credentials" src_ip="1.1.1.1" message="User priyanka failed to login to VPN portal through Local authentication mechanism because of wrong credentials" name="" src_mac=""
17720	messageid="17720" log_type="Event" log_component="VPN Portal Authentication" log_subtype="Authentication" status="Successful" user="priyanka" user_group="" client_used="N/A" auth_mechanism="N/A" reason="" src_ip="10.166.71.2" message="User priyanka logged out of VPN portal" name="" src_mac=""

DDNS

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - DDNS: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - DDNS: Log Type = Event & Log Subtype = System & Log Component = DDNS

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is CR_*ddns_log_fmt*.

Syslog field name	Data type	Length	Format /Description	Possible values	Notes/Examples
Timestamp	Timestamp		ISO 8601		eg. Timestamp="2018-12-07T10:03:48+0000"
device_name	String			SFW	eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="063711517815"
log_component	String		component of log	DDNS	e.g. log_component=DDNS
log_type	String			Event	eg. log_type="Event"
log_subtype	String		subtype of log	System	e.g. log_subtype=System
log_version	Number			1	eg. log_version=1
severity	String		severity of event	Notification	e.g. severity="Notification"
status	String				eg. status="Successful"
src_host	String	256	hostname for ddns		e.g. src_host="xyz.firewall.co"
reported_ip					
reason	String	128	reason of event failure	Invalid Response Invalid IP Invalid Configuration or bad authorization Unknown Error DNS Error Reported Abuse Invalid Response Connect Failed	

message	String	1024			e.g. message="DDNS update for host test1.customtest.dyndns.org was Successful. Updated with IP 10.198.232.86." message="DDNS update for host test1.customtest.dyndns.org was Failed. Last Updated with IP:10.198.232.86

Sample logs

Message ID	Log
17815	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is *ddns_log_fmt*.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes/Examples
log_type	log_type	log_type	u_int8_t	8	log type	Event	e.g. log_type=Event
log_component	log_component	log_component	u_int8_t	8	component of log	DDNS	e.g. log_component=DDNS
log_subtype	log_subtype	log_subtype	u_int8_t	8	subtype of log	System	e.g. log_subtype=System
priority	severity		u_int8_t	8	severity of event	Notification	e.g. severity="Notification"
host	hostname	host	String	256	hostname for ddns		e.g. hostname="xyz.firewall.co"
updatedip		updated_ip					
reason	failure_reason	reason	String	128	reason of event failure	Invalid Response Invalid IP Invalid Configuration or bad authorization Unknown Error DNS Error Reported Abuse Invalid Response Connect Failed	
message		message	String	1024			e.g. message="DDNS update for host test1.customtest.dyndns.org was Successful. Updated with IP 10.198.232.86." message="DDNS update for host test1.customtest.dyndns.org was Failed. Last Updated with IP:10.198.232.86

Sample logs

Message ID	Log
17815	`device="SFW" date=2018-06-06 time=11:12:10 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=063711517815 log_type="Event" log_component="DDNS" log_subtype="System" status="Success" priority=Notice host=test1.customtest.dyndns.org updatedip=10.198.232.86 reason="" message="DDNS update for host test1.customtest.dyndns.org was Successful. Updated with IP 10.198.232.86."`

DHCP server

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - DHCP Server: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - DHCP Server: Log Type = Event & Log Subtype = System & Log Component = DHCP Server

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is CR_*dhcp_svr_log_fmt*.

Syslog field name	Data type	Length	Format/Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String			SFW	eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="010101600001"
log_type	String		Log Type	Event	
log_component	String		Log Component	DHCP Server	e.g. log_component="DHCP Server"
log_subtype	String		Log subtype	System	e.g. log_subtype="System"
status	String		DHCP lease status	Renew Release Expire	e.g. status="Renew"
log_version	Number			1	eg. log_version=1
Severity	String		Severity of log	Information	
reported_ip			IPv4 or IPv6 address leased to DHCP client		e.g. reported_ip="55.1.1.2"
src_mac	String	32	MAC address of the DHCP client		e.g. src_mac="1a:74:ed:3c:74:ce"
reported_host	String	384	Hostname of the DHCP client		e.g. reported_host="AH-MM-33445.green.sophos"
message	String	1024	Message about DHCP lease		e.g. message="Lease IP 55.1.1.2 renewed for MAC 1a:74:ed:3c:74:ce"
lease_time	Number				eg. lease_time=86400

Sample logs

Message ID	Log

60020	
60021	
60022	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is *dhcp_svr_log_fmt*.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type		log_type	String		Log Type	Event	
log_component		log_component	String		Log Component	DHCP Server	e.g. log_component="DHCP Server"
log_subtype		log_subtype	String		Log subtype	System	e.g. log_subtype="System"
status		status	String		DHCP lease status	Renew Release Expire	e.g. status="Renew"
priority			String		Priority of log	INFORMATION	
ipaddress		leased_ip			IPv4 or IPv6 address leased to DHCP client		e.g. leased_ip="55.1.1.2"
client_physical_address		src_mac	String	32	MAC address of the DHCP client		e.g. src_mac="1a:74:ed:3c:74:ce"
client_host_name		client_host_name	String	384	Hostname of the DHCP client		e.g. client_host_name="AH-MM-33445.green.sophos"
message		message	String	1024	Message about DHCP lease		e.g. message="Lease IP 55.1.1.2 renewed for MAC 1a:74:ed:3c:74:ce"
raw_data		raw_data		8192	DHCP lease details		e.g. raw_data="55.1.1.2 Tue 05 Jun 00:51:06 2018 Wed 06 Jun 00:51:06 2018 1a:74:ed:3c:74:ce -

Sample logs

Message ID	Log
60020	`device="SFW" date=2018-06-04 time=21:25:36 timezone="-03" device_name="XG330" device_id=C310073YJRGBF7F log_id=063411660020 log_type="Event" log_component="DHCP Server" log_subtype="System" status="Renew" priority=Information ipaddress="5.5.5.5" client_physical_address="00:1a:8c:5f:b4:f6" client_host_name="" message="Lease IP 5.5.5.5 renewed for MAC 00:1a:8c:5f:b4:f6" raw_data="5.5.5.5#011Mon 04 Jun 21:25:36 2018#011Mon 04 Jun 21:27:36 2018#01100:1a:8c:5f:b4:f6#011-"`
60021	`device="SFW" date=2018-06-04 time=21:34:22 timezone="-03" device_name="XG330" device_id=C310073YJRGBF7F log_id=063411660021 log_type="Event" log_component="DHCP Server" log_subtype="System" status="Release" priority=Information ipaddress="5.5.5.15" client_physical_address="00:1a:8c:5f:b4:f6" client_host_name="" message="Lease IP 5.5.5.15 released from MAC 00:1a:8c:5f:b4:f6" raw_data="5.5.5.15#01100:1a:8c:5f:b4:f6#011-"`

60022	device="SFW" date=2018-06-04 time=21:34:22 timezone="-03" device_name="XG330" device_id=C310073YJRGBF7F log_id=063411660022 log_type="Event" log_component="DHCP Server" log_subtype="System" status="Expire" priority=Information leased_ip="172.16.16.17" src_mac="-" client_host_name="" message="Lease 172.16.16.17 expired" raw_data="172.16.16.17"

Email (antispam)

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - Email Usage: Reports > Email > Email Usage
  - Email Spam: Reports > Email > Email Protection
- Log identifier for reports:
  - Email Usage: Log Component = (SMTP or POP3 or IMAP4 or SMTPS or POPS or IMAPS) & Log Subtype = (Allowed or Clean or Outbound Clean or DLP or SPX)
  - Email Spam: Log Component = (SMTP or POP3 or IMAP4 or SMTPS or POPS or IMAPS) & Log Subtype = (Spam or Probable Spam or Outbound Spam or Outbound Probable Spam)

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is CR_*mail_as_log_fmt*.

Syslog field name	Data type	Length	Format /Description	Possible values	Notes/Examples
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String				eg. device_name="SFW"
device_model	String				eg. device_model="XG135"
device_serial_id	String				eg. device_serial_id="C44313350024-P29PUA"
log_id	String				eg. log_id="041107413001"
log_type			Log type	Anti-Spam	
log_component			Component of log	SMTP SMTPS	
log_subtype			Type of spam	Spam Probable Spam Clean Outbound Spam Outbound Probable Spam Outbound Clean DLP SPX Dos Allowed Denied	
log_version	Number			1	eg. log_version=1
severity			Severity of mail spam	Information Warning Notification Error	

fw_rule_id	Number	int32			
user_name	String	384			
user_group	String				eg. user_group="student"
policy_name	String	32	Policy name		
sender	String	1024	Email address of sender		e.g. sender="test@test.local"
recipient	String	1024	Email address of recipient		eg. recipient="test1@test.local"
subject	String	1024	Subject of mail		eg. subject="test"
message_id	String	64	Message id		eg. message_id="10001"
email_size	u_int32_t	int32	Message size		eg. email_size="1111"
action	String	32		Drop Quarantine Reject Tmpreject Accept	
reason	String	256		Mail detected as SPAM Mail detected as PROBABLE SPAM Mail is Clean Sender IP address is blacklisted Mail detected as OUTBOUND SPAM Mail detected as OUTBOUND PROBABLE SPAM Email containing confidential data detected. Relevant Data Protection Policy applied. SMTP DoS	
src_host	String	64			
dst_host	String	64			
src_ip	ipaddr_t	32	Source IP address		eg. src_ip="1.1.1.1" src_ip="345::12"
src_country	String	64	ISO 3166 (A 3) Code		eg. "IND" "USA"
dst_ip	ipaddr_t	32	Destination IP address		eg. dst_ip="1.1.1.2" dst_ip="345::11"
dst_country	String	64	ISO 3166 (A 3) Code		eg. "IND" "USA"
src_port	u_int16_t	16	Source port		eg. src_port="1234"
dst_port	u_int16_t	16	Destination port		eg. dst_port="12345"
protocol	String				eg. protocol="POP"
src_zone_type	String				eg. src_zone_type="LAN"
src_zone	String				eg. src_zone="LAN"
dst_zone_type	String				eg. dst_zone_type="WAN"
dst_zone	String				eg. dst_zone="WAN"
bytes_sent	Number	int32			
bytes_received	Number	int32			

quarantine_reason	u_int32_t	32	Reason for mail quarantine		eg. quarantine_reason="Infected"
app_name	String				

Sample logs

Message ID	Log
13001	
13002	
13003	
13004	
13005	
13006	
13007	obsolete
13008	obsolete
13009	
13010	
13011	
13012	
13013	
13014	
14001	
14002	
14003	
15001	
15002	
15003	
18035	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is *mail_as_log_fmt*.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes/Examples
log_type	log_type	log_type	u_int8_t		Log type	Anti-Spam	
log_component	log_component	log_component	u_int8_t		Component of log	SMTP SMTPS	

log_subtype	log_subtype	log_subtype	u_int8_t		Type of spam	Spam Probable Spam Clean Outbound Spam Outbound Probable Spam Outbound Clean DLP SPX Dos Allowed Denied	
priority	severity		u_int8_t		Severity of mail spam	Information Warning Notification Error	
fw_rule_id		fw_rule_id	Number	int32			
user_name		user	String	384			
av_policy_name	avaspolicy	policy_name	String	32	Policy name		
from_email_address	sender	sender	String	1024	Email address of sender		e.g. sender="test@test.local"
to_email_address	rcpts	recipient	String	1024	Email address of recipient		eg. rcpts="test1@test.local"
email_subject	subject	subject	String	1024	Subject of mail		eg. subject="test"
mailid	messageid	message_id	String	64	Message id		eg. messageid="10001"
mailsize	mail_size	email_size	u_int32_t	int32	Message size		eg. mail_size="1111"
spamaction		action	String	32		Drop Quarantine Reject Tmpreject Accept	
reason		reason	String	256		Mail detected as SPAM Mail detected as PROBABLE SPAM Mail is Clean Sender IP address is blacklisted Mail detected as OUTBOUND SPAM Mail detected as OUTBOUND PROBABLE SPAM Email containing confidential data detected. Relevant Data Protection Policy applied. SMTP DoS	
src_domainname		host	String	64			
dst_domainname		domain	String	64			
src_ip	src_ip	src_ip	ipaddr_t	32	Source IP address		eg. src_ip="1.1.1.1" src_ip="345::12"
src_country_code		src_country	String	64	Source country code		eg. "IND" "USA"
dst_ip	dst_ip	dst_ip	ipaddr_t	32	Destination IP address		eg. dst_ip="1.1.1.2" dst_ip="345::11"

dst_country_code		dst_country	String	64	Destination country code		eg. "IND" "USA"
src_port	src_port	src_port	u_int16_t	16	Source port		eg. src_port="1234"
dst_port	dst_port	dst_port	u_int16_t	16	Destination port		eg. dst_port="12345"
sent_bytes		bytes_sent	Number	int32			
recv_bytes		bytes_received	Number	int32			
quarantine_reason	reason	quarantine_reason	u_int32_t	32	Reason for mail quarantine		eg. quarantine_reason="Infected"

Sample logs

Message ID	Log
13001	device="SFW" date=2017-01-31 time=18:28:25 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=041107413001 log_type="Anti-Spam" log_component="SMTP" log_subtype="Spam" status="" priority=Warning fw_rule_id=0 user_name="gaurav" av_policy_name="Gaurav235" from_email_address="gaurav1@iview.com" to_email_address="gaurav2@iview.com" email_subject="RPD Spam Test: Spam" mailid="c000000b-1485867502" mailsize=400 spamaction="DROP" reason="" src_domainname="iview.com" dst_domainname="" src_ip=10.198.47.71 src_country_code=R1 dst_ip=10.198.233.61 dst_country_code=R1 protocol="TCP" src_port=22258 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Spam"
13002	device="SFW" date=2018-06-06 time=10:41:29 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041108413002 log_type="Anti-Spam" log_component="SMTP" log_subtype="Probable Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="postman" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" email_subject="[SPAM] RPD Spam test: Bulk" mailid="c0000006-1528261885" mailsize=438 spamaction="WARN" reason="Mail detected as PROBABLE SPAM." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.16.204 dst_country_code=R1 protocol="TCP" src_port=56341 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Spam"
13003	device="SFW" date=2017-01-31 time=18:36:22 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=041105613003 log_type="Anti-Spam" log_component="SMTP" log_subtype="Clean" status="" priority=Information fw_rule_id=0 user_name="gaurav" av_policy_name="None" from_email_address="gaurav2@iview.com" to_email_address="gaurav1@iview.com" email_subject="EMAIL" mailid="<5ab27db7-7bac-82e2-ba40-83ce90577c7f@iview.com>" mailsize=398 spamaction="Accept" reason="" src_domainname=" iview.com" dst_domainname="" src_ip=10.198.47.71 src_country_code=R1 dst_ip=10.198.233.61 dst_country_code=R1 protocol="TCP" src_port=22477 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
13004	device="SFW" date=2018-06-06 time=11:08:08 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041108413004 log_type="Anti-Spam" log_component="SMTP" log_subtype="Probable Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="postman" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" email_subject="Test RBL email" mailid="c0000008-1528263488" mailsize=433 spamaction="DROP" reason="Sender IP address is blacklisted." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.17.121 dst_country_code=R1 protocol="TCP" src_port=57854 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="RBL"
13005	device="SFW" date=2017-01-31 time=18:34:41 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=041113413005 log_type="Anti-Spam" log_component="SMTP" log_subtype="Outbound Spam" status="" priority=Warning fw_rule_id=0 user_name="gaurav" av_policy_name="Gaurav123" from_email_address="gaurav1@iview.com" to_email_address="gaurav2@iview.com" email_subject="RPD Spam Test: Spam" mailid="<a22c9da6-19e5-4764-2836-3f48d7dcc329@iview.com>" mailsize=405 spamaction="Accept" reason="" src_domainname=" iview.com" dst_domainname="" src_ip=10.198.47.71 src_country_code=R1 dst_ip=10.198.233.61 dst_country_code=R1 protocol="TCP" src_port=22420 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Spam"

13006	device="SFW" date=2018-06-06 time=11:10:11 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041114413006 log_type="Anti-Spam" log_component="SMTP" log_subtype="Outbound Probable Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="rule 8" from_email_address="pankhil@postman.local" to_email_address="pankhil1@Postman.local" email_subject="RPD Spam test: Bulk" mailid="<c63b1eb2-1c17-73ac-fcc3-20e8831dc3d3@postman.local>" mailsize=439 spamaction="Drop" reason="Mail detected as OUTBOUND PROBABLE SPAM." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.234.240 dst_country_code=R1 protocol="TCP" src_port=58043 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Spam"
13007	obsolete
13008	obsolete
13009	device="SFW" date=2018-06-06 time=12:50:07 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041121613009 log_type="Anti-Spam" log_component="SMTP" log_subtype="DLP" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="postman" from_email_address="pankhil@postman.local" to_email_address="pankhil1@Postman.local" email_subject="Fwd: TESt" mailid="c0000002-1528269606" mailsize=5041 spamaction="DROP" reason="Email containing confidential data detected. Relevant Data Protection Policy applied." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.17.121 dst_country_code=R1 protocol="TCP" src_port=60134 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="DLP"
13010	device="SFW" date=2018-06-06 time=12:51:34 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041122613010 log_type="Anti-Spam" log_component="SMTP" log_subtype="SPX" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="pankhil1@Postman.local" email_subject="[secure:pankhil]" mailid="c0000003-1528269693" mailsize=442 spamaction="Accept" reason="SPX Template of type Specified by Sender successfully applied on Email." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.16.204 dst_country_code=R1 protocol="TCP" src_port=60298 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
13011	device="SFW" date=2018-06-06 time=12:52:49 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041122613011 log_type="Anti-Spam" log_component="SMTP" log_subtype="SPX" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="pankhil1@Postman.local" email_subject="Test failed" mailid="c0000004-1528269769" mailsize=431 spamaction="REJECT" reason="Email could not be SPX-encrypted because password was not found in the Email subject." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.16.204 dst_country_code=R1 protocol="TCP" src_port=60305 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
13012	device="SFW" date=2018-06-06 time=12:53:39 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041123413012 log_type="Anti-Spam" log_component="SMTP" log_subtype="Dos" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="" to_email_address="" email_subject="" mailid="" mailsize=0 spamaction="TMPREJECT" reason="SMTP DoS" src_domainname="" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.17.121 dst_country_code=R1 protocol="TCP" src_port=60392 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
13013	device="SFW" date=2017-01-31 time=15:46:45 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=041101613013 log_type="Anti-Spam" log_component="SMTP" log_subtype="Allowed" status="" priority=Information fw_rule_id=0 user_name="gaurav" av_policy_name="Gaurav235" from_email_address="gaurav2@iview.com" to_email_address="gaurav1@iview.com" email_subject="GP235" mailid="c000000a-1485857789" mailsize=391 spamaction="SANDSTORM ALLOW" reason="Mail is marked Clean by Sophos Sandstorm." src_domainname="iview.com" dst_domainname="" src_ip=10.198.47.71 src_country_code=R1 dst_ip=10.198.233.61 dst_country_code=R1 protocol="TCP" src_port=11255 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
13014	device="SFW" date=2018-06-06 time=12:56:53 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041102413014 log_type="Anti-Spam" log_component="SMTP" log_subtype="Denied" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="postman" from_email_address="pankhil1@postman.local" to_email_address="pankhil@postman.local" email_subject="Fwd: test sand" mailid="c0000008-1528270010" mailsize=419835 spamaction="DROP" reason="Email is marked Malicious by Sophos Sandstorm." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.17.121 dst_country_code=R1 protocol="TCP" src_port=60608 dst_port=25 sent_bytes=0 recv_bytes=0

14001	device="SFW" date=2017-01-31 time=18:31:11 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=041207414001 log_type="Anti-Spam" log_component="POP3" log_subtype="Spam" status="" priority=Warning fw_rule_id=0 user_name="gaurav" av_policy_name="GauravPatel" from_email_address="gaurav1@iview.com" to_email_address="gaurav2@iview.com" email_subject="RPD Spam Test: Spam" mailid="<2a2dd5d4-1a30-617b-27b1-7961ad07cf07@iview.com>" mailsize=574 spamaction="Accept" reason="" src_domainname=" iview.com" dst_domainname="iview.com" src_ip=10.198.47.71 src_country_code=R1 dst_ip=10.198.233.61 dst_country_code=R1 protocol="TCP" src_port=22333 dst_port=110 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
14002	device="SFW" date=2018-06-06 time=12:59:01 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=046108414002 log_type="Anti-Spam" log_component="POPS" log_subtype="Probable Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="pop8" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" email_subject="RPD Spam test: Bulk" mailid="<13c3aad0-82c0-11d8-c9e1-3c0ea4f8708b@postman.local>" mailsize=0 spamaction="Change Subject" reason="Mail detected as PROBABLE SPAM" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code= dst_ip=10.198.234.240 dst_country_code= protocol="TCP" src_port=60742 dst_port=995 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
14003	device="SFW" date=2018-06-06 time=13:00:34 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=046105614003 log_type="Anti-Spam" log_component="POPS" log_subtype="Clean" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" email_subject="Test clean" mailid="<b4ac9385-437d-7cd1-1089-ef09fb3066fa@postman.local>" mailsize=0 spamaction="Accept" reason="Mail is Clean" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code= dst_ip=10.198.234.240 dst_country_code= protocol="TCP" src_port=60757 dst_port=995 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
15001	device="SFW" date=2018-06-06 time=13:01:42 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=046207415001 log_type="Anti-Spam" log_component="IMAPS" log_subtype="Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="ganga@postman.local" email_subject="RPD Spam test: Spam" mailid="<6da55e70-8d61-63fb-df41-35fdf36e94d8@postman.local>" mailsize=0 spamaction="Accept" reason="Mail detected as SPAM" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code= dst_ip=10.198.234.240 dst_country_code= protocol="TCP" src_port=58595 dst_port=993 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
15002	device="SFW" date=2018-06-06 time=13:02:54 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=046208415002 log_type="Anti-Spam" log_component="IMAPS" log_subtype="Probable Spam" status="" priority=Warning fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="ganga@postman.local" email_subject="RPD Spam test: Bulk" mailid="<0a09a814-f3b6-35cc-c94e-1807dab742fc@postman.local>" mailsize=0 spamaction="Accept" reason="Mail detected as PROBABLE SPAM" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code= dst_ip=10.198.234.240 dst_country_code= protocol="TCP" src_port=58595 dst_port=993 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
15003	device="SFW" date=2018-06-06 time=13:03:58 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=046205615003 log_type="Anti-Spam" log_component="IMAPS" log_subtype="Clean" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="ganga@postman.local" email_subject="Clean email" mailid="<3b542388-7bca-5b43-79e6-e21fcd709d8f@postman.local>" mailsize=0 spamaction="Accept" reason="Mail is Clean" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code= dst_ip=10.198.234.240 dst_country_code= protocol="TCP" src_port=58595 dst_port=993 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
18035	device="SFW" date=2018-06-05 time=19:11:26 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=041101618035 log_type="Anti-Spam" log_component="SMTP" log_subtype="Allowed" status="" priority=Information fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="pankhil@Postman.local" email_subject="dd" mailid="c0000005-1528206082" mailsize=421 spamaction="DELIVERED" reason="Email has been delivered to recipient(s)." src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.16.204 dst_country_code=R1 protocol="TCP" src_port=61636 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"

Email (antivirus)

Log format name under crformatter.conf is `mail_av_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	log_type	log_type	u_int8_t	8	log type	Anti-virus	
log_component	log_component	log_component	u_int8_t	8	component of log	SMTP SMTPS	
log_subtype	log_subtype	log_subtype	u_int8_t	8	subtype of log	Virus	
priority	severity		u_int8_t		severity of mail virus	Critical	
fw_rule_id	fw_rule_id	fw_rule_id	Number	int32			
user_name		user					
av_policy_name	avaspolicy	policy_name	String	32	policy name		eg. avaspolicy="policy1"
from_email_address	sender	sender	String	1024	email address of sender		eg. sender="test@test.local"
to_email_address	rcpts	recipient	String	1024	email address of recipient		eg. rcpts="test1@test.local"
subject	subject	subject	String	1024	subject of mail		eg. subject="test"
mailid	messageid	message_id	String	64	message id		eg. messageid="10001"
mailsize	mail_size	email_size	u_int32_t	int32	mail size		eg. mail_size="1111"
virus	virusname	virus	String	32	virus name		eg. virusname="eicar"
filename	qname	file_name	String	64	file name		eg. qname="QBin.2/1960x2000000c.eml_0_1524566566"
quarantine	qname	quarantine	String	64	quarantine file name		eg. qname="QBin.2/1960x2000000c.eml_0_1524566566"
src_domainname		host					
dst_domainname		domain					
src_ip	src_ip	src_ip	ipaddr_t	32	source ip address		eg. src_ip="1.1.1.1",src_ip="345::12"
src_country_code		src_country					
dst_ip	dst_ip	dst_ip	ipaddr_t	32	destination ip address		eg. dst_ip="1.1.1.2",dst_ip="345::11"
dst_country_code		dst_country					
src_port	src_port	src_port	u_int16_t	16	source port		eg. src_port="12345"
dst_port	dst_port	dst_port	u_int16_t	16	destination port		eg. dst_port="12345"
sent_bytes		bytes_sent					
recv_bytes		bytes_received					
quarantine_reason	reason	quarantine_reason	u_int32_t	32	reason for mail quarantine		eg. quarantine_reason="Infected" quarantine_reason="Mail Unscannable"

Reporting

- Reports under>
  - Email Usage: Reports > Email > Email Usage
  - Email Virus: Reports > Email > Email Protection
- Log identifier for reports>
  - Email Usage: Log Component = (SMTP or POP3 or IMAP4 or SMTPS or POPS or IMAPS) & Log Subtype = (Allowed or Clean or Outbound Clean or DLP or SPX)
  - Email Virus: Log Component = (SMTP or POP3 or IMAP4 or SMTPS or POPS or IMAPS) & Log Subtype = Virus

Sample logs

Message ID	Log
10001	device="SFW" date=2018-06-06 time=10:44:40 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=031106210001 log_type="Anti-Virus" log_component="SMTP" log_subtype="Virus" status="" priority=Critical fw_rule_id=0 user_name="" av_policy_name="postman" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" subject="virus infected message" mailid="c0000007-1528262079" mailsize=2064 virus="EICAR-AV-Test" filename="" quarantine="" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.17.121 dst_country_code=R1 protocol="TCP" src_port=56428 dst_port=25 sent_bytes=0 recv_bytes=0 quarantine_reason="Infected"
~~10002~~	Not found in the code.
11001	device="SFW" date=2018-06-06 time=10:51:29 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=036106211001 log_type="Anti-Virus" log_component="POPS" log_subtype="Virus" status="" priority=Critical fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="pankhil@postman.local" subject="EICAR" mailid="<a5c35e4b-1198-d0eb-0763-c0d5af3c817e@postman.local>" mailsize=0 virus="EICAR-AV-Test" filename="" quarantine="" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.234.240 dst_country_code=R1 protocol="TCP" src_port=56653 dst_port=995 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
~~11002~~	Not found in the code.
12001	device="SFW" date=2018-06-06 time=10:58:29 timezone="IST" device_name="SG430" device_id=S4000806149EE49 log_id=036206212001 log_type="Anti-Virus" log_component="IMAPS" log_subtype="Virus" status="" priority=Critical fw_rule_id=0 user_name="" av_policy_name="None" from_email_address="pankhil@postman.local" to_email_address="ganga@postman.local" subject="EICAR test email" mailid="<2ca37b7c-e93a-743a-99c4-a0796f0bbb79@postman.local>" mailsize=0 virus="EICAR-AV-Test" filename="" quarantine="" src_domainname="postman.local" dst_domainname="" src_ip=10.198.16.121 src_country_code=R1 dst_ip=10.198.234.240 dst_country_code=R1 protocol="TCP" src_port=56632 dst_port=993 sent_bytes=0 recv_bytes=0 quarantine_reason="Other"
~~12002~~	Not found in the code.

Email quarantine

Log format name under crformatter.conf is *quarantine_log_fmt*.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	log_type	log_type	u_int8_t	8		Event	
log_component		log_component	u_int8_t	8		Quarantine	
log_subtype		log_subtype	u_int8_t	8		System	
priority	severity		u_int8_t		8	Severity of mail	
subject	subject	subject	String	1024	subject of mail		e.g. subject="test"
from	sender	sender	String	1024	email address of sender		e.g. sender="test@test.local"
to	rcpts	recipient	String	1024	email address of recipient		e.g. rcpts="test1@test.local"
message		message	String	1024			

Reporting

- Reports under:
  - Quarantine Event: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - Quarantine Event: Log Type = Event & Log Subtype = System

Sample logs

Message ID	Log
17823	Obsolete

Firewall

Log format name under crformatter.conf is `firewall_log_fmt`.

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Examples/Notes
log_type	log_type	String	8	Log Type	Firewall	
log_component	log_component	String	8	Log Component	Firewall Rule Heartbeat ICMP ERROR MESSAGE Invalid Traffic Fragmented Traffic Invalid Fragmented Traffic Local ACL DoS Attack ICMP Redirection Source Routed MAC Filter IPMAC Filter IP Spoof SSL VPN Virtual Host	
log_subtype	log_subtype	String	8	Log sub type	Allowed Denied Drop	
status	status	String	8	Status of log	Allow Deny	
priority		String	8	Priority of log	Warning Notification Information	
duration	con_duration	Number	int32	Time between the start and close of connection		
fw_rule_id	fw_rule_id	Number	int32	Rule ID used for particular request		
policy_type	policy_type	Number	int8	Firewall template (network / user / business policy)		
user_name	user	String	384	Client login username		
user_gp	user_group	String	1024	User group detail		
iap	web_policy_id	Number	int16	Id of Web policy applied		
ips_policy_id	ips_policy_id	Number	int16	Id of IPS policy applied		
appfilter_policy_id	appfilter_policy_id	Number	int16	Id of application filter applied		
application	app_name	String	64	Application name at client machine		
application_risk	app_risk	Number	8	Defined risk level (1-5)		
application_technology	app_technology	String	32	Technology of application		eg. "Browser Based" "P2P" "Client Server" "Network Protocol"

application_category	app_category	String	64	Category in which application belong		eg. "Streaming Media" "Web Mail" "Social Networking" "File Transfer" "Network Services"
in_interface	in_interface	String	64	In interface name of traffic of firewall		eg. PortA
out_interface	out_interface	String	64	Out interface name of traffic of firewall		eg. PortB
src_mac	src_mac	String	32	Client source mac address		
dst_mac	dst_mac	String	32	Destination mac address		
vlan_id	vlan_id	Number	16	Vlan id		
src_ip	src_ip	ipaddr_t		Client source ip address		
src_country_code	src_country	String	64	Client source country code		eg. "IND","USA" etc
dst_ip	dst_ip	ipaddr_t		Destination IP address		
dst_country_code	dst_country	String	64	Destination country code		eg. "IND","USA" etc
src_port	src_port	Number		Source port number		
dst_port	dst_port	Number		Destination port number		
icmp_type	icmp_type	String		ICMP Type	Refer to ICMP protocol details for possible values	eg. 8 - Echo 0 - Echo Reply, etc
icmp_code	icmp_code	String		ICMP Code	Refer to ICMP protocol details for possible values	
sent_pkts	packets_sent	Number	int32	Number of packets sent		
recv_pkts	packets_received	Number	int32	Number of packets received		
sent_bytes	bytes_sent	Number	int32	Number of bytes sent		
recv_bytes	bytes_received	Number	int32	Number of bytes received		
tran_src_ip	src_trans_ip	ipaddr_t		Translated source IP (Nat source IP)		
tran_src_port	src_trans_port			Translated source port (Nat source port)		
tran_dst_ip	dst_trans_ip	ipaddr_t		Translated destination IP (Nat destination IP)		
tran_dst_port	dst_trans_port			Translated destination Port (Nat destination Port)		
srczonetype	src_zone_type	String	int32	Type of custom zone (LAN or DMZ)		
srczone	src_zone	String	64 bits	SFOS Source Zone	LAN WAN DMZ VPN WiFi Custom	
dstzonetype	dst_zone_type	String	int32	Type of custom zone (LAN or DMZ)		
dstzone	dst_zone	String	64 bits	SFOS Destination Zone		
dir_disp	con_direction	String		Direction of connection		
connevent	con_event	String		Connection Event	Start Interim Stop	
connid	con_id	Number	int32	Connection ID		
vconnid	virt_con_id	Number	int32	Master connection ID (in case of related connections)		

hb_health	hb_status	Number	int16	Endpoint Heartbeat status	No Heartbeat Green Yellow Red Missing	
message	message	String	1024	Message about particular packet		eg. message="Invalid UDP destination."
appresolvedby	appresolvedby	String		Module via which client application name is resolved	Signature EAC Proxy	EAC = Enhanced App Control (Synchronised Application)
app_is_cloud	app_is_cloud	Number	int16	Set if application is web/cloud based	0 1	

ether_type	ether_type	Number	int16	Specifies the ethernet frame type	{0x0000, "Unknown"}, { 0x00FE, "GRE-OSI" }, { 0x0200, "PUP" }, { 0x0500, "Sprite" }, { 0x0600, "NS" }, { 0x0707, "GeoNet (old)" }, { 0x0800, "IPv4" }, { 0x0806, "ARP" }, { 0x0842, /*Wake-on-LAN*/ "Wake-on-LAN" }, { 0x1000, "Trail" }, { 0x22EA, /*Stream Reservation Protocol*/ "SRP" }, { 0x22F0, /*Audio Video Transport Protocol (AVTP)*/ "AVTP" }, { 0x22F3, /*IETF TRILL Protocol*/ "TRILL" }, { 0x6001, "MOP DL" }, { 0x6002, /*DEC MOP RC*/"MOP RC" }, { 0x6003, /*DECnet Phase IV, DNA Routing*/"DN" }, { 0x6004, /*DEC LAT*/"LAT" }, { 0x6007, "SCA" }, { 0x6558, "TEB" }, { 0x8035, "Reverse ARP" }, { 0x8038, "Lanbridge" }, { 0x803c, "DEC DNS" }, { 0x803e, "DEC DTS" }, { 0x805b, "VEXP" }, { 0x805c, "VPROD" }, { 0x809b, "Appletalk" }, { 0x80f3, "Appletalk ARP" }, { 0x8100, "802.1Q" }, { 0x8102, /*Simple Loop Prevention Protocol (SLPP)*/ "SLPP" }, { 0x8137, "IPX" }, { 0x8204, /*QNX Qnet*/ "QNX Qnet" }, { 0x86dd, "IPv6" }, { 0x8808, "MPCP" }, { 0x8809, "Slow Protocols" }, { 0x880b, "PPP" }, { 0x8819, /*CobraNet*/ "Cobranet" }, { 0x8847, "MPLS unicast" }, { 0x8848, "MPLS multicast" }, { 0x8863, "PPPoE D" }, { 0x8864, "PPPoE S" }, { 0x886D, /*Intel Advanced Networking Services*/ "IANS" }, { 0x886f, "MS NLB heartbeat" }, { 0x8870, "Jumbo" }, { 0x887B, /*HomePlug 1.0 MME*/ "HomePlug 1.0 MME" }, { 0x888e, "EAPOL" }, { 0x8892, /*PROFINET Protocol*/ " PROFINET" }, { 0x8899, "RRCP" }, { 0x889A, /*HyperSCSI (SCSI over Ethernet)*/ "HyperSCSI" }, { 0x88A4, /*EtherCAT Protocol*/ "EtherCAT" }, { 0x88a8, "802.1Q-QinQ" }, { 0x88AB, /*Ethernet Powerlink*/ "Ethernet Powerlink" }, { 0x88B8, /*GOOSE (Generic Object Oriented Substation event) */ "GOOSE" }, { 0x88B9, /*GSE (Generic Substation Events) Management Services*/ "GSE" }, { 0x88BA, /*SV (Sampled Value Transmission)*/ "SV" }, { 0x88ca, "TIPC" }, { 0x88cc, "LLDP" }, { 0x88CD, /*SERCOS III*/ "SERCOS III" }, { 0x88DC, /*WSMP, WAVE Short Message Protocol*/ "WSMP" }, { 0x88E1, /*HomePlug AV MME*/ "HomePlug AV MME" }, { 0x88E3, /*Media Redundancy Protocol (IEC62439-2)*/ "MRP" }, { 0x88E5, /*MAC security (IEEE 802.1AE)*/ "MAC security" }, { 0x88E7, /*Provider Backbone Bridges (PBB) (IEEE 802.1ah)*/ "PBB" }, { 0x88F7, /*Precision Time Protocol (PTP) over Ethernet (IEEE 1588)*/ "PTP" }, { 0x88F8, /*NC-SI*/ "NC-SI" }, { 0x88FB, /*Parallel Redundancy Protocol (PRP)*/ "PRP" }, { 0x8902, "CFM" }, { 0x8906, /*Fibre Channel over Ethernet (FCoE)*/ "FCoE" }, { 0x8914, /*FCoE Initialization Protocol*/ "FCoE initialization" }, { 0x8915, /*RDMA over Converged Ethernet (RoCE)*/ "RoCE" }, { 0x891D, /*TTEthernet Protocol Control Frame (TTE)*/ "TTE" }, { 0x892F, /*High-availability Seamless Redundancy (HSR)*/ "HSR" }, { 0x893a, "IEEE1905.1" }, { 0x8947, "GeoNet" }, { 0x894F, "NSH" }, { 0x9000, "Loopback" }, { 0x9100, "802.1Q-9100" }, { 0x9200, "802.1Q-9200" }, { 0xabcd, "CFM (old)" }, { 0xCAFE, /*Veritas Technologies Low Latency Transport (LLT) */ "LLT" }, { 0xfefe, "OSI" }	
sdwan_profile_id_request	sdwan_profile_id_request	Number	uint16	SD-WAN profile id for request direction		
sdwan_profile_name_request	sdwan_profile_name_request	String		SD-WAN profile name for request direction.		
sdwan_profile_id_reply	sdwan_profile_id_reply	Number	uint16	SD-WAN profile id for reply direction		
sdwan_profile_name_reply	sdwan_profile_name_reply	String		SD-WAN profile name for reply direction		
gw_id_request	gw_id_request	Number	uint16	ID of gateway used for request direction		

gw_name_request	gw_name_request	String		Name of gateway used for request direction		
gw_id_reply	gw_id_reply	Number	uint16	ID of gateway used for reply direction		
gw_name_reply	gw_name_reply	String		Name of gateway used for reply direction		
sdwan_route_id_request	sdwan_route_id_request	Number	uint32	SD-WAN route id used in request direction		
sdwan_route_name_request	sdwan_route_name_request	String		SD-WAN route name used in request direction		
sdwan_route_id_reply	sdwan_route_id_reply	Number	uint32	SD-WAN route id used in reply direction		
sdwan_route_name_reply	sdwan_route_name_reply	String		SD-WAN route name used in reply direction		

Reporting

- Reports under:
  - Application Allowed: Reports > Application & Web > User App Risks & Usage
  - Also use to report:
    - CASB (With combination of Web Logs): Reports > Application & Web > Cloud Application Usage
    - Synchronised Application (Where appresolvedby = EAC) : Reports > Application & Web > Synchronized Application
    - Security Heartbeat (When Log Component = Heartbeat) : Reports > Network & Threats > Security Heartbeat
- Log identifier for reports:
  - Application Allowed: Log Type = Firewall & Log Component = Firewall Rule & Log Subtype = Allowed

Sample logs

Message ID	Log
1	device="SFW" date=2021-05-13 time=07:23:19 timezone="IST" device_name="SF01V" device_id=SFDemo-ta-vm-205 log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=5 nat_rule_id=2 policy_type=1 sdwan_profile_id_request=1 sdwan_profile_name_request=SDWAN_Profile_Test sdwan_profile_id_reply=0 sdwan_profile_name_reply= gw_id_request=2 gw_name_request=gw0 gw_id_reply=0 gw_name_reply= sdwan_route_id_request=1 sdwan_route_name_request=PBR_SDWANTest sdwan_route_id_reply=0 sdwan_route_name_reply= user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" vlan_id="" ether_type=Unknown (0x0000) bridge_name="" bridge_display_name="" in_interface="Port4" in_display_interface="Port4" out_interface="Port1" out_display_interface="Port1" src_mac=00:50:56:B0:9F:2C dst_mac=00:50:56:B0:3D:3D src_ip=10.171.113.55 src_country_code=R1 dst_ip=10.171.65.129 dst_country_code=R1 protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=10.171.0.197 tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="LAN" srczone="LAN" dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="1486087634" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0 log_occurrence=1
2	device="SFW" date=2018-05-30 time=13:14:26 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010102600002 log_type="Firewall" log_component="Firewall Rule" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=1 policy_type=1 user_name="" user_gp="" iap=2 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port1" out_interface="Port2.531" src_mac=b8:97:5a:5b:0f:fd src_ip=10.198.32.19 src_country_code= dst_ip=8.8.8.8 dst_country_code= protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature

3	device="SFW" date=2018-06-01 time=10:55:41 timezone="BST" device_name="XG310" device_id=SFDemo-9a04c43 log_id=016602600003 log_type="Firewall" log_component="Heartbeat" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=16 policy_type=1 user_name="" user_gp="" iap=2 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port3.611" out_interface="" src_mac=08:00:27:4c:49:e3 src_ip=10.198.37.57 src_country_code= dst_ip=72.163.4.185 dst_country_code= protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="Red" message="" appresolvedby="Signature" app_is_cloud=0
4	device="SFW" date=2018-05-30 time=17:55:09 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=018202500004 log_type="Firewall" log_component="ICMP ERROR MESSAGE" log_subtype="Denied" status="Deny" priority=Notice duration=0 fw_rule_id=1 policy_type=1 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port2.531" out_interface="" src_mac=00:1a:8c:50:6a:8c src_ip=120.72.91.145 src_country_code= dst_ip=10.198.232.48 dst_country_code= protocol="ICMP" icmp_type=11 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="1084482152" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
5	device="SFW" date=2018-05-30 time=18:03:43 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=018201500005 log_type="Firewall" log_component="ICMP ERROR MESSAGE" log_subtype="Allowed" status="Allow" priority=Notice duration=0 fw_rule_id=1 policy_type=1 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port2.531" out_interface="" src_mac=00:1a:8c:50:6a:8c src_ip=172.29.250.33 src_country_code= dst_ip=10.198.232.48 dst_country_code= protocol="ICMP" icmp_type=11 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connevent="Interim" connid="14310965" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
6	device="SFW" date=2018-06-01 time=10:57:55 timezone="BST" device_name="XG310" device_id=SFDemo-9a04c43 log_id=016602600006 log_type="Firewall" log_component="Heartbeat" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=16 policy_type=1 user_name="" user_gp="" iap=2 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port3.611" out_interface="" src_mac=08:00:27:4c:49:e3 src_ip=10.198.37.57 src_country_code= dst_ip=10.198.32.19 dst_country_code= protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="Red" message="" appresolvedby="Signature" app_is_cloud=0
~~7~~	Not found in code.
1001	device="SFW" date=2018-05-30 time=13:26:37 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010202601001 log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="" out_interface="" src_mac= src_ip=10.198.32.19 src_country_code= dst_ip=8.8.8.8 dst_country_code= protocol="UDP" src_port=1353 dst_port=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="Invalid UDP destination." appresolvedby="Signature"
1301	device="SFW" date=2018-06-04 time=17:20:24 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=011402601301 log_type="Firewall" log_component="Fragmented Traffic" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="" out_interface="" src_mac= src_ip=0.0.0.0 src_country_code= dst_ip=0.0.0.0 dst_country_code= protocol="0" src_port=0 dst_port=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"

~~1601~~	Not found in code. The following relevant invalid traffic is generated for Invalid Fragmented Traffic: device="SFW" date=2018-06-05 time=18:27:04 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010202601001 log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port2.611" out_interface="" src_mac=b8:97:5a:5b:0f:fd src_ip=10.198.36.184 src_country_code= dst_ip=10.198.36.48 dst_country_code= protocol="TCP" src_port=1417 dst_port=444 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="Invalid IP fragment." appresolvedby="Signature"
~~2001~~	Not found in code.
2002	device="SFW" date=2018-05-30 time=14:01:32 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010302602002 log_type="Firewall" log_component="Appliance Access" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=2 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port2.611" out_interface="" src_mac=c8:5b:76:ab:72:d3 src_ip=10.198.38.184 src_country_code= dst_ip=10.198.39.255 dst_country_code= protocol="UDP" src_port=137 dst_port=137 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
3001	device="SFW" date=2018-05-30 time=14:17:17 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010402403001 log_type="Firewall" log_component="DoS Attack" log_subtype="Denied" status="Deny" priority=Warning duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port1" out_interface="" src_mac=b8:97:5a:5b:0f:fd src_ip=10.198.32.19 src_country_code= dst_ip=10.198.32.48 dst_country_code= protocol="TCP" src_port=41960 dst_port=22 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
4001	device="SFW" date=2018-06-05 time=14:30:31 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010502604001 log_type="Firewall" log_component="ICMP Redirection" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="" out_interface="" src_mac= src_ip=10.198.37.23 src_country_code= dst_ip=10.198.36.48 dst_country_code= protocol="ICMP" icmp_type=5 icmp_code=1 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
5001	device="SFW" date=2018-05-31 time=17:05:14 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=010602605001 log_type="Firewall" log_component="Source Routed" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=1 policy_type=1 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="" out_interface="" src_mac= src_ip=10.198.12.19 src_country_code= dst_ip=8.8.8.8 dst_country_code= protocol="TCP" src_port=1571 dst_port=80 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
5051	device="SFW" date=2018-05-30 time=15:09:51 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=011702605051 log_type="Firewall" log_component="MAC Filter" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port2.531" out_interface="" src_mac=1e:3a:5a:5b:23:ab src_ip=fe80::59f5:3ce8:c98e:5062 src_country_code= dst_ip=ff02::1:2 dst_country_code= protocol="UDP" src_port=546 dst_port=547 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"

5101	device="SFW" date=2018-05-30 time=15:12:45 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=011802605101 log_type="Firewall" log_component="IPMAC Filter" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="Port1" out_interface="" src_mac=b8:97:5a:5b:0f:fd src_ip=10.198.32.15 src_country_code= dst_ip=216.58.196.174 dst_country_code= protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
5151	device="SFW" date=2018-05-30 time=14:04:25 timezone="IST" device_name="XG125w" device_id=SFDemo-763180a log_id=011902605151 log_type="Firewall" log_component="IP Spoof" log_subtype="Denied" status="Deny" priority=Information duration=0 fw_rule_id=0 policy_type=0 user_name="" user_gp="" iap=0 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" in_interface="" out_interface="" 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 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="" srczone="" dstzonetype="" dstzone="" dir_disp="" connid="" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature"
~~5201~~	Not found in code.
~~5401~~	Not found in code.
0001	device="SFW" date=2020-06-05 time=03:45:23 timezone="CEST" device_name="SF01V" device_id=SFDemo-ta-vm-55 log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=5 nat_rule_id=2 policy_type=1 user_name="" user_gp="" iap=13 ips_policy_id=0 appfilter_policy_id=0 application="" application_risk=0 application_technology="" application_category="" vlan_id="" ether_type=Unknown (0x0000) bridge_name="" bridge_display_name="" in_interface="Port2" in_display_interface="Port2" out_interface="Port1" out_display_interface="Port1" src_mac=00:50:56:99:51:94 dst_mac=00:50:56:99:3D:AC src_ip=10.146.13.30 src_country_code= dst_ip=10.8.142.181 dst_country_code= protocol="TCP" src_port=45294 dst_port=443 sent_pkts=0 recv_pkts=0 sent_bytes=0 recv_bytes=0 tran_src_ip=10.8.13.110 tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczonetype="LAN" srczone="LAN" dstzonetype="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="2674291981" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0 log_occurrence=1

Gateway

Log format name under crformatter.conf is *gateway_log_fmt*.

Field descriptions

Syslog Field Name	LogViewer Detail-View Field Name	Data Type	Length	Format /Description	Possible Values	Examples/Notes
log_type	log_type	String		Log Type	Event	
log_component	log_component	String		Log Component	Gateway	
log_subtype	log_subtype	String		Log sub type	System	
priority		String		Priority of log	Notice	
gatewayname	gw_name		8192	Gateway Name		e.g. gw_name="DHCP_Port2_GW"
message	message	String	1024	Event Message		e.g. message="Gateway DHCP_Port2_GW is Up"

Reporting

- Reports under:
  - Gateway: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - Gateway: Log Type = Event & Log Subtype = System & Log Component = Gateway

Sample logs

Message ID	Log

17814	`device="SFW" date=2018-06-05 time=02:55:45 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063611517814 log_type="Event" log_component="Gateway" log_subtype="System" priority=Notice gatewayname="DHCP_Port2_GW" message="Gateway DHCP_Port2_GW is Up"`
	
	`device="SFW" date=2018-06-05 time=02:55:45 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063611517814 log_type="Event" log_component="Gateway" log_subtype="System" priority=Notice gatewayname="DHCP_Port2_GW" message="Gateway DHCP_Port2_GW is Down"`

HA - High availability

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
device	N/A	N/A				SFW	Not exposed in log viewer
date	Time	date and time are combined in log viewer field			YYYY-MM-DD The system-local date/time at which the event occurred		
time	Time				hh:mm:ss 24-hour format	"09:48:48"	
timezone	N/A	N/A					e.g. timezone="CET" Not exposed in log viewer
device_name	N/A	N/A	String	16	Appliance model name		e.g. device_name="XG125w" Not exposed in log viewer
device_id	N/A	N/A	String	32	Appliance's serial ID		e.g. device_id=C44313350024-P29PUA Not exposed in log viewer
log_type	log_type	log_type	String			Event	
log_component		log_component	String			HA	
log_subtype		log_subtype	String			System	
priority			String			Notice	
status	N/A	status	String				

Reporting

- Reports under:
  - HA: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - HA: Log Type = Event & Log Subtype = System & Log Component = HA

HA message logs

Message ID	Log	Log Type	Log Component	Log Subtype	Severity
60012	Appliance becomes standalone	Event	HA	System	Notification
60013	Appliance goes in fault	Event	HA	System	Notification
60014	Appliance becomes auxiliary	Event	HA	System	Notification
60015	Appliance becomes primary	Event	HA	System	Notification
60016	Appliance becomes standalone at appliance start up	Event	HA	System	Notification
60017	Appliance goes in fault at appliance start up	Event	HA	System	Notification
60018	Appliance becomes auxiliary at appliance start up	Event	HA	System	Notification
60019	Appliance becomes primary at appliance start up	Event	HA	System	Notification
60023	HA System: Dedicated interface is unplugged, please check your HA System	Event	HA	System	Warning
60024	HA System: Monitor interface/s is/are unplugged, please check your HA System	Event	HA	System	Warning
17838	HA was disabled	Event	HA	System	Notification

Sample logs

Message ID	Log message
60012	device="SFW" date=2021-07-17 time=09:48:48 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f2 log_id=061611560012 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=SFDemo-qa-vcluster-sf1-f2 message="Appliance with appliance key SFDemo-qa-vcluster-sf1-f2 becomes standalone"
60013	device="SFW" date=2018-06-05 time=12:56:37 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560013 log_type="Event" log _component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B goes in fault"
60014	device="SFW" date=2018-06-05 time=15:06:51 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560014 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B becomes auxiliary"
60015	device="SFW" date=2021-07-17 time=09:51:06 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f2 log_id=061611560015 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=SFDemo-qa-vcluster-sf1-f2 message="Appliance with appliance key SFDemo-qa-vcluster-sf1-f2 becomes primary"
60016	device="SFW" date=2018-06-05 time=09:05:18 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560016 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B becomes standalone at appliance startup"
60017	device="SFW" date=2018-06-05 time=15:07:01 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560017 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B goes in fault at appliance startup"
60018	device="SFW" date=2021-07-17 time=09:51:01 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f1 log_id=061611560018 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=SFDemo-qa-vcluster-sf1-f1 message="Appliance with appliance key SFDemo-qa-vcluster-sf1-f1 becomes auxiliary at appliance startup"
60019	device="SFW" date=2018-06-05 time=09:11:18 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611560019 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="Appliance with appliance key C30006CBC4838C2 becomes primary at appliance startup"
60023	device="SFW" date=2021-07-19 time=11:42:27 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f2 log_id=061611560023 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="" Appliance_Key=SFDemo-qa-vcluster-sf1-f2 message="Interface Port4 went down. Appliance HA state MAST"
60024	device="SFW" date=2021-07-19 time=13:13:39 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f2 log_id=061611560024 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="" Appliance_Key=SFDemo-qa-vcluster-sf1-f2 message="Interface Port2 went down. Appliance HA state MAST" device="SFW" date=2021-07-19 time=13:17:36 timezone="EDT" device_name="SF01V" device_id=SFDemo-qa-vcluster-sf1-f2 log_id=061611560024 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="" Appliance_Key=SFDemo-qa-vcluster-sf1-f2 message="Interface Port2 went down. Appliance HA state BACK"
17838	device="SFW" date=2018-06-05 time=09:11:18 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611517838 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="HA was disabled because firmware upgrade to auxiliary appliance with appliance key S210055D2BDFDDD failed. Firmware successfully upgraded on primary appliance with appliance key C30006CBC4838C2"

Heartbeat

Log format name under crformatter.conf is `hb_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type	log_type	log_type	String			Heartbeat	
log_component		log_component	String			Heartbeat	
log_subtype		log_subtype	String			Information	
priority			String			Information	
RED		red	Number	int32	total number of endpoints in state RED		2
YELLOW		yellow	Number	int32	total number of endpoints in state YELLOW		3
GREEN		green	Number	int32	total number of endpoints in state GREEN		4
TOTAL		total	Number	int32	total number of endpoints in total		500

Reporting

- Not capture for reporting
- Log identifier for reports:
  - Heartbeat Endpoint: Log Type = Heartbeat & Log Component = Heartbeat

Sample logs

Message ID	Log
18012	

Heartbeat endpoint

Log format name under crformatter.conf is `ep_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	log_type	log_type	String			Heartbeat	Heartbeat
log_component		log_component	String			Endpoint	Endpoint
log_subtype		log_subtype	String			Information	Information
priority			String			Notice	Notice
ep_name	Endpoint Name	Endpoint Name	String	1028	Netbios Name of the endpoint	Whatever microsoft allows FIM-WIN7-PC3	• FIM-WIN7-PC3 • Heartbeat206-PC
ep_uuid	endpoint_id	endpoint_id	String	40	UUID of this endpoint - created on Sophos Central		• 54d320ef-7c6c-4cc7-b900-8aabcc9ca04b
ep_ip	endpoint_ip	endpoint_ip	String	15	IP address of the endpoint		172.16.10.33
ep_health	Endpoint Health	Endpoint Health	String	12	Health state of the endpoint	• Disconnected • Green • Yellow • Red • Missing	
ep_event_time	ep_event_time		unix time stamp		Time when this event was triggered from EP		• 1485950078 • 1485948707

Reporting

- Reports under:
  - Heartbeat Endpoint: Reports > Network & Threats > Security Heartbeat
- Log identifier for reports:
  - Heartbeat Endpoint: Log Type = Heartbeat & Log Component = Endpoint

Sample logs

Message ID	Log
18013	`device="SFW" date=2017-02-01 time=17:01:55 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=116725518013 log_type="Heartbeat" log_component="Endpoint" log_subtype="Information" priority=Notice ep_name=Heartbeat206-PC ep_uuid=54d320ef-7c6c-4cc7-b900-8aabcc9ca04b ep_ip=10.198.47.206 ep_health=Green ep_event_time=1485948715`  `device="SFW" date=2017-02-01 time=17:01:47 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=116725518013 log_type="Heartbeat" log_component="Endpoint" log_subtype="Information" priority=Notice ep_name=Heartbeat206-PC ep_uuid=54d320ef-7c6c-4cc7-b900-8aabcc9ca04b ep_ip=10.198.47.206 ep_health=Red ep_event_time=1485948707`  `device="SFW" date=2017-02-01 time=17:24:38 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=116725518013 log_type="Heartbeat" log_component="Endpoint" log_subtype="Information" priority=Notice ep_name=Heartbeat206-PC ep_uuid=54d320ef-7c6c-4cc7-b900-8aabcc9ca04b ep_ip=10.198.47.206 ep_health=Missing ep_event_time=1485950078`

Interface

Log format name under crformatter.conf is `interface_log_fmt`.

Field descriptions

Syslog Field Name	Name	LogViewer Detail-View Field Name	Data Type	Length	Format /Description	Possible Values	Examples/Notes
log_type		log_type	String		Log Type	Event	
log_component		log_component	String		Log Component	Interface	
log_subtype		log_subtype	String		Log sub type	System	
priority			String		Log priority	Information, Notice	
interface		interface	String	32	Interface Name		e.g. interface="PortA"
message		message	String	1024	Event message		e.g. message="Interface Port1 is Up" message="Interface Port1 is Down"

Reporting

- Reports under:
  - Interface: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - Interface: Log Type = Event & Log Subtype = System & Log Component = Interface

Sample logs

Message ID	Log

17813	`device="SFW" date=2018-06-05 time=02:52:56 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063511617813 log_type="Event" log_component="Interface" log_subtype="System" priority=Information interface="Port2" message="Interface Port2 is Down"`
	
	`device="SFW" date=2018-06-05 time=02:53:00 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063511617813 log_type="Event" log_component="Interface" log_subtype="System" priority=Information interface="Port2" message="Interface Port2 is Up"`

17820	`device="SFW" date=2018-06-05 time=03:10:58 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063511517820 log_type="Event" log_component="Interface" log_subtype="System" priority=Notice interface="Port5" message="Primary link Port5 is Down"`
	
	`device="SFW" date=2018-06-05 time=03:10:58 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=063511517820 log_type="Event" log_component="Interface" log_subtype="System" priority=Notice interface="Port5" message="Primary link Port5 is Up"`

19030	messageid="19030" log_type="Event" log_component="Interface" log_subtype="System" interface="" display_interface="" message="IPv6 prefix 2a01:db8:3::/56 delegated by ISP to Port2." messageid="19030" log_type="Event" log_component="Interface" log_subtype="System" interface="" display_interface="" message="Lease expired for delegated IPv6 prefix 2a01:db8:3::/56 assigned to Port2."
17502	messageid="17502" log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" user="admin" src_ip="10.198.39.254" additional_information="" message="PortF13 set to no breakout by 'admin' from '10.198.39.254' using 'GUI'" messageid="17502" log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" user="admin" src_ip="10.198.39.254" additional_information="" message="PortF13 set to 2-port breakout by 'admin' from '10.198.39.254' using 'GUI'" messageid="17502" log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" user="admin" src_ip="10.198.39.254" additional_information="" message="PortF13 set to 4-port breakout by 'admin' from '10.198.39.254' using 'GUI'"

17504	messageid="17504" log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" user="admin" src_ip="10.166.71.1" additional_information="" message="Interface 'Port4' was turned on by 'admin' from '10.166.71.1' using 'GUI'" messageid="17504" log_type="Event" log_component="GUI" log_subtype="Admin" status="Successful" user="admin" src_ip="10.166.71.1" additional_information="" message="Interface 'Port4' was turned off by 'admin' from '10.166.71.1' using 'GUI'"

IPS

Log format name under crformatter.conf is `idp_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type		log_type	String			IDP	
log_component		log_component	String			Anomaly Signatures	
log_subtype		log_subtype	String			Detect Drop	
priority			String			Warning	
idp_policy_id		ips_policy_id	Number	int16	Id of the IPS Policy configured		
fw_rule_id		fw_rule_id	Number	int32	Firewall rule id		
user_name		user	String	384			
signature_id		sig_id	Number	int32	sid of the IPS signature triggered		
signature_msg		message	String	128	msg of the IPS signature triggered		
classification		classification	String	64	classification based on the classtype of the IPS signature triggered		
rule_priority		rule_priority	Number	int8	Priority of the rule within the Policy		
src_ip		src_ip					
src_country_code		src_country	String	64	Source country code		eg. "IND" "USA" etc
dst_ip		dst_ip					
dst_country_code		dst_country	String	64	Destination country code		eg. "IND" "USA" etc
src_port		src_port					
dst_port		dst_port					
icmp_type		icmp_type					
icmp_code		icmp_code					
platform		OS	String	512	Platform in which Signature is classified	Platforms present in IPS signature set	
category		category	String	1024	Category in which signature is classfied	Categories present in IPS signature set	
target		victim	String	128	Target in which signature is classified	Targets present in IPS signature set	

Reporting

- Reports under:
  - IPS : Reports > Network & Threats > Intrusion Attacks
- Log identifier for reports:
  - IPS : Log Type = IDP & Log Component = (Anomaly or Signatures)

Sample logs

Message ID	Log

6001	device="SFW" date=2018-05-23 time=16:20:34 timezone="BST" device_name="XG750" device_id=SFDemo-f64dd6be log_id=020703406001 log_type="IDP" log_component="Anomaly" log_subtype="Detect" priority=Warning idp_policy_id=1 fw_rule_id=2 user_name="" signature_id=26022 signature_msg="FILE-PDF EmbeddedFile contained within a PDF" classification="A Network Trojan was detected" rule_priority=1 src_ip=10.0.0.168 src_country_code=R1 dst_ip=10.1.1.234 dst_country_code=R1 protocol="TCP" src_port=28938 dst_port=25 platform="Windows" category="Malware Communication" target="Server"
6002	device="SFW" date=2018-05-23 time=16:16:43 timezone="BST" device_name="XG750" device_id=SFDemo-f64dd6be log_id=020704406002 log_type="IDP" log_component="Anomaly" log_subtype="Drop" priority=Warning idp_policy_id=1 fw_rule_id=2 user_name="" signature_id=26022 signature_msg="FILE-PDF EmbeddedFile contained within a PDF" classification="A Network Trojan was detected" rule_priority=1 src_ip=10.0.1.31 src_country_code=R1 dst_ip=10.1.0.115 dst_country_code=R1 protocol="TCP" src_port=40140 dst_port=25 platform="Windows" category="Malware Communication" target="Server"
7001	device="SFW" date=2018-05-23 time=15:49:38 timezone="BST" device_name="XG750" device_id=SFDemo-f64dd6be log_id=020803407001 log_type="IDP" log_component="Signatures" log_subtype="Detect" priority=Warning idp_policy_id=1 fw_rule_id=2 user_name="" signature_id=584 signature_msg="PROTOCOL-RPC portmap rusers request UDP" classification="Decode of an RPC Query" rule_priority=5 src_ip=10.0.1.39 src_country_code=R1 dst_ip=10.1.0.42 dst_country_code=R1 protocol="UDP" src_port=21378 dst_port=111 platform="BSD,Linux,Mac,Solaris,Unix" category="Operating System and Services" target="Server"
7002	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"

IPsec

Log format name under crformatter.conf is `ipsec_log_fmt`.

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes/Examples
log_type	log_type	String			Event	
log_component	log_component	String			IPSec	
log_subtype	log_subtype	String			System	
priority	priority	String			Alert Critical Error Warning Notice Information Debug	"Alert"
user_name	user_name	String	384			xauth username
connectionname	connectionname	String	32			If the connectionname is longer, it will be trunacted to 32 characters.
connectiontype	connectiontype	Number	int8		0	unused
localinterfaceip	localinterfaceip					"153.25.15.25"
localgateway	gw_ip					Next hop of the localinterfaceip
localnetwork	local_network	String	32			"10.8.48.0/24"
remoteinterfaceip	dst_ip					"153.25.15.25"
remotenetwork	remote_network	String	32			"10.8.49.0/24"
message	message	String	1024			

Reporting

- Reports under:
  - IPsec: Reports > VPN > VPN
  - Also use to report:
    - Reports > Compliance > Events > System Events
- Log identifier for reports:
  - IPsec: Log Type = Event & Log Subtype = System & Log Component = IPSec

Sample logs

Message ID	Log
17801	`messageid="17801" log_type="Event" log_component="IPSec" log_subtype="System" status="Established" user="" con_name="rr-1" con_type="0" src_ip="10.171.4.118" gw_ip="" local_network="2.2.2.2/32" dst_ip="10.171.4.117" remote_network="1.1.1.1/32" additional_information="" message="rr-1 - IPSec Connection rr-1 between 10.171.4.117 and 10.171.4.118 for Child rr-1 established. (Remote: 10.171.4.117)"`

17802	messageid="17802" log_type="Event" log_component="IPSec" log_subtype="System" status="Terminated" user="" con_name="rr-1" con_type="0" src_ip="10.171.4.118" gw_ip="" local_network="2.2.2.2/32" dst_ip="10.171.4.117" remote_network="1.1.1.1/32" additional_information="" message="rr-1 - IPSec Connection rr-1 between 10.171.4.117 and 10.171.4.118 for Child rr-1 terminated. (Remote: 10.171.4.117)"
18044	messageid="18044" log_type="Event" log_component="IPSec" log_subtype="System" status="Disconnected" user="" con_name="" con_type="0" src_ip="" gw_ip="" local_network="" dst_ip="" remote_network="" additional_information="" message="RADIUS request message timed out."
18045	messageid="18045" log_type="Event" log_component="IPSec" log_subtype="System" status="Disconnected" user="" con_name="" con_type="0" src_ip="" gw_ip="" local_network="" dst_ip="" remote_network="" additional_information="" message="Received shutdown signal (2)."
18046	messageid="18046" log_type="Event" log_component="IPSec" log_subtype="System" status="Deny Session" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Couldn't authenticate the local gateway. Check the authentication settings on both devices. (Remote: 10.171.4.118)"
18047	messageid="18047" log_type="Event" log_component="IPSec" log_subtype="System" status="Deny Session" user="" con_name="Ipsec_res-1" con_type="0" src_ip="10.171.4.118" gw_ip="" local_network="" dst_ip="10.171.4.117" remote_network="" additional_information="" message="Ipsec_res-1 - Couldn't authenticate the remote gateway . Check the authentication settings on both devices. (Remote: 10.171.4.117)"
18048	messageid="18048" log_type="Event" log_component="IPSec" log_subtype="System" status="Deny Session" user="" con_name="IPSec_new_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="IPSec_new_ini-1 - Couldn't resolve the remote gateway IP address. Check the gateway configuration on both devices. (Remote: 10.171.4.118)"
18049	messageid="18049" log_type="Event" log_component="IPSec" log_subtype="System" status="Deny Session" user="" con_name="IPSec_new_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="IPSec_new_ini-1 - Remote gateway didn't respond to the initial message %u. Check if the remote gateway is reachable. (Remote: 10.171.4.118)"
18050	messageid="18050" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="IPSec_new_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Received IKE message with invalid SPI (61ADBCD7) from the remote gateway."
18051	messageid="18051" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="IPSec_new_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="IPSec_new_ini-1 - Couldn't parse IKE header from 10.171.4.117. Check the debug logs.(Remote: 10.171.4.118)"
18052	messageid="18052" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="IPSec_new_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="IPSec_new_ini-1 - Couldn't parse IKE message from 10.171.4.118[500]. Check the debug logs. ((Remote: 10.171.4.118)"
18053	severity is DEBUG so it will not be seen in the garner
18054	severity is DEBUG so it will not be seen in the garner
18055	messageid="18055" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - IKE message (34001D60) retransmission to 10.171.4.118 timed out. Check if the remote gateway is reachable. (Remote: 10.171.4.118)"
18056	GARNER doesn't handle this ALERT
18057	messageid="18057" log_type="Event" log_component="IPSec" log_subtype="System" status="Expire" user="" con_name="" con_type="0" src_ip="" gw_ip="" local_network="" dst_ip="" remote_network="" additional_information="" message="Couldn't establish IKE_SA: Timed out. Remote gateway aborted the IKE exchange or the message was lost. Check the remote device logs."

18058	messageid="18058" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - IKE SA proposals don't match. Check the phase 1 policy settings on both devices: IKE:AES_CBC_256 /HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/CURVE_25519, IKE:AES_CBC_256/HMAC_SHA2_384_192 /PRF_HMAC_SHA2_384/CURVE_25519, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/CURVE_25519, IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/ECP_521, IKE:AES_CBC_256/HMAC_SHA2_384_192 /PRF_HMAC_SHA2_384/ECP_521, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_521, IKE: AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/ECP_256, IKE:AES_CBC_256/HMAC_SHA2_384_192 /PRF_HMAC_SHA2_384/ECP_256, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/ECP_256, IKE: AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_8192, IKE:AES_CBC_256/HMAC_SHA2_384_192 /PRF_HMAC_SHA2_384/MODP_8192, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/MODP_8192, IKE: AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SHA2_512/MODP_4096, IKE:AES_CBC_256/HMAC_SHA2_384_192 /PRF_HMAC_SHA2_384/MODP_4096, IKE:AES_CBC_256/HMAC_SHA2_256_128/PRF_HMAC_SHA2_256/"
18059	messageid="18059" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - CHILD_SA proposals don't match. Check the phase 2 policy settings on both devices: ESP:AES_CBC_256 /HMAC_SHA2_512_256/MODP_4096/NO_EXT_SEQ (Remote: 10.171.4.118)"
18060	messageid="18060" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="IPsec_ini-1" con_type="0" src_ip="10.171.4.118" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="IPsec_ini-1 - Traffic selectors don't match. Check the configured local and remote subnets on both devices: 1.1.1.1/32 === 2.2.2.2/32 (Remote: 10.171.4.118)"
18061	GARNER doesn't handle this ALERT
18062	messageid="18062" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Couldn't install IPsec policy. (Remote: 10.171.4.118)"
18063	messageid="18063" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Couldn't install IPsec SA. (Remote: 10.171.4.118)"
18064	message="Replaced existing IKE_SA due to uniqueness policy." .Not reproduced
18065	message="Retained the existing IKE_SA instead of the rejected one due to uniqueness policy.". Not reproduced
18066	GARNER doesn't handle this ALERT
18067	message="Couldn't allocate a virtual IP address. Requested address: 1.1.1.1" Not reproduced
18068	message="XAUTH: Couldn't authenticate the user. Incorrect username or password." Not reproduced
18069	messageid="18069" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Certificate expired. Issuer: 'C=CA, ST=Ontario, L=Ottawa, O=Sophos, OU=OU, CN=Default_CA_18X6Qn6tsr4vJEL, E=na@example.com', validity: Jun 17 22:49:59 UTC 4443530 to Jun 17 22:36:32 UTC 4443530" (Remote: 10.171.4.118)"
18070	messageid="18070" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Certificate revoked. Issuer: 'C=CA, ST=Ontario, L=Ottawa, O=Sophos, OU=OU, CN=Default_CA_18X6Qn6tsr4vJEL, E=na@example.com' (Remote: 10.171.4.118)"
18071	GARNER doesn't handle this ALERT
18072	messageid="18072" log_type="Event" log_component="IPSec" log_subtype="System" status="Failed" user="" con_name="Ipsec_ini-1" con_type="0" src_ip="10.171.4.117" gw_ip="" local_network="" dst_ip="10.171.4.118" remote_network="" additional_information="" message="Ipsec_ini-1 - Certificate isn't from a trusted authority: 'C=CA, ST=Ontario, L=Ottawa, O=Sophos, OU=OU, CN=Default_CA_18X6Qn6tsr4vJEL, E=na@example.com' (Remote: 10.171.4.118)"
18073	GARNER doesn't handle this ALERT

18074	GARNER doesn't handle this ALERT
18075	GARNER doesn't handle this ALERT
18076	These are not ALERTS. These are submodules
18077	These are not ALERTS. These are submodules
18078	These are not ALERTS. These are submodules
18079	These are not ALERTS. These are submodules
18080	These are not ALERTS. These are submodules
18081	These are not ALERTS. These are submodules
18082	These are not ALERTS. These are submodules
18083	These are not ALERTS. These are submodules
18084	These are not ALERTS. These are submodules
18085	These are not ALERTS. These are submodules
18086	These are not ALERTS. These are submodules
18087	These are not ALERTS. These are submodules
18088	These are not ALERTS. These are submodules
18089	These are not ALERTS. These are submodules
18090	These are not ALERTS. These are submodules
18091	These are not ALERTS. These are submodules
18092	These are not ALERTS. These are submodules
18093	These are not ALERTS. These are submodules
18094	These are not ALERTS. These are submodules

IPsec failover

Log format name under crformatter.conf is `ipsec_failover_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type		log_type	String			Event	
log_component		log_component	String			IPSec	
log_subtype		log_subtype	String			System	
priority			String				
message		message	String	1024			

Reporting

- Reports under:
  - IPSec: Reports > VPN > VPN
  - Also use to report:
    - Reports > Compliance > Events > System Events
- Log identifier for reports:
  - IPSec: Log Type = Event & Log Subtype = System & Log Component = IPSec

Sample logs

Message ID	Log
17832	
17833	
17834	
17835	
17836	
17837	

L2TP PPTP VPN

Log format name under crformatter.conf is `l2tp_pptp_log_fmt` (this is used by OPCODE updown_vpn_event).

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes /Examples
log_type	log_type	String			Event	
log_component	log_component	String			L2TP PPTP	
log_subtype	log_subtype	String			System	
priority		String			Notice Information	see below
user_name	user	String	384			see below
localip	src_ip					see below
remotepeer	dst_ip					see below
ipleased	leased_ip					see below
reason	reason	String	64		""	see below
bytes_sent	bytes_sent	Number	int32			see below
bytes_recv	bytes_received	Number	int32			see below
message	message	String	1024		"User $username was $state successfully through $vpncomp using leased IP $leasediphb" $state : terminated, established $vpncomp: pptp, l2tp	see below

Reporting

- Reports under:
  - L2TP PPTP VPN: Reports > VPN > VPN
  - Also use to report:
    - Reports > Compliance > Events > System Events
- Log identifier for reports:
  - Access Gateway: Log Type = Event & Log Subtype = System & Log Component = (L2TP or PPTP)

Sample logs

Message ID	Log
17803	`device="SFW" date=2017-03-15 time=14:33:37 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062611617803 log_type="Event" log_component="L2TP" log_subtype="System" status="Established" priority=Information user_name="gaurav" localip=10.198.233.48 remotepeer=10.198.233.49 ipleased=192.168.1.1 reason="" bytes_sent=159326560 bytes_recv=159326560 message="User gaurav was established successfully through l2tp using leased IP 192.168.1.1"`
17804	`device="SFW" date=2017-03-15 time=14:53:11 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062611517804 log_type="Event" log_component="L2TP" log_subtype="System" status="Terminated" priority=Notice user_name="gaurav" localip=10.198.233.48 remotepeer=10.198.233.49 ipleased=192.168.1.1 reason="" bytes_sent=1277545 bytes_recv=138967 message="User gaurav was terminated successfully through l2tp using leased IP 192.168.1.1"`

17805	device="SFW" date=2017-03-15 time=16:13:33 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062711617805 log_type="Event" log_component="PPTP" log_subtype="System" status="Established" priority=Information user_name="gaurav" localip=10.198.233.48 remotepeer=10.198.233.49 ipleased=192.168.2.1 reason="" bytes_sent=155727280 bytes_recv=155727280 message="User gaurav was established successfully through pptp using leased IP 192.168.2.1"
17806	device="SFW" date=2017-03-15 time=16:14:00 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062711517806 log_type="Event" log_component="PPTP" log_subtype="System" status="Terminated" priority=Notice user_name="gaurav" localip=10.198.233.48 remotepeer=10.198.233.49 ipleased=192.168.2.1 reason="" bytes_sent=16682 bytes_recv=18475 message="User gaurav was terminated successfully through pptp using leased IP 192.168.2.1"

RED

Log format name under crformatter.conf is `red_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes/Examples
log_type		log_type	String			Event	
log_component		log_component	String			RED	
log_subtype		log_subtype	String			System	
priority			String				
red_id		red_id	String	64	RED10: A32XXXX XXXXXXXX RED15: A35XXXX XXXXXXXX RED15W: A36XXXXXXXXXXX RED50: A34XXXX XXXXXXXX Server: XXXXXXX XXXXXXXX		This is the ID of the RED. The first 3 digits describes the type of the RED, and the last 12 digits are alphanumeric digits. For red server there are 15 alphanumeric digits.
status		status	String			Connected Disconnected Interim	
eventtime	Event Time	event_time					
duration		duration	Number	int32			Describes the time in ms between a disconnect and a reconnect of the machine. Only for connect messages else zero.
branch_name		branch_name	String	64			Name of the red device in the redconfig.
recv_bytes		bytes_received	Number	int32			Bytes recevied by the device
sent_bytes		bytes_sent	Number	int32			Bytes send from the device
message		message	String	1024	<RED_ID>/<branch name> message		Message from the device with either the RX/TX or the a connect /disconnect message

Reporting

- Reports under:
  - RED: Reports > VPN > VPN
- Log identifier for reports:
  - RED: Log Type = Event & Log Component = RED & Log Subtype = System

Sample logs

Message ID	Log
18014	`device="SFW" date=2017-03-16 time=12:56:01 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618014 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Connected" eventtime="2017-03-16 12:56:01 IST" duration=164000 branch_name=Gaurav Patel recv_bytes=0 sent_bytes=0 message="A350196C47072B0/Gaurav Patel is now re-connected after 164000 ms"`

18015	device="SFW" date=2017-03-16 time=12:53:29 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618015 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Disconnected" eventtime="2017-03-16 12:53:29 IST" duration=0 branch_name=Gaurav Patel recv_bytes=32256 sent_bytes=22844 message="A350196C47072B0/Gaurav Patel is now disconnected" device="SFW" date=2017-03-16 time=12:53:27 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618015 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Disconnected" eventtime="2017-03-16 12:53:27 IST" duration=0 branch_name=Gaurav Patel recv_bytes=31488 sent_bytes=22368 message="A350196C47072B0/Gaurav Patel is now disconnected" device="SFW" date=2017-03-16 time=12:47:50 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618015 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Disconnected" eventtime="2017-03-16 12:47:50 IST" duration=0 branch_name=NY recv_bytes=0 sent_bytes=0 message="A350196C47072B0/NY is now disconnected" device="SFW" date=2017-03-16 time=12:46:33 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618015 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Disconnected" eventtime="2017-03-16 12:46:33 IST" duration=0 branch_name=NY recv_bytes=180180384 sent_bytes=127851012 message="A350196C47072B0/NY is now disconnected"
18016	device="SFW" date=2017-03-16 time=12:59:34 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618016 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Interim" eventtime="2017-03-16 12:59:34 IST" duration=0 branch_name=Gaurav Patel recv_bytes=41472 sent_bytes=29372 message="A350196C47072B0/Gaurav Patel transfered bytes TX: 41472 RX: 29372" device="SFW" date=2017-03-16 time=12:46:26 timezone="IST" device_name="XG125w" device_id=S1601E1F9FCB7EE log_id=066811618016 log_type="Event" log_component="RED" log_subtype="System" priority=Information red_id=A350196C47072B0 status="Interim" eventtime="2017-03-16 12:46:26 IST" duration=0 branch_name=NY recv_bytes=0 sent_bytes=0 message="A350196C47072B0/NY transfered bytes TX: 0 RX: 0"

Sandstorm events

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_sandbox_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Sandbox	
log_component	Log Comp	log_component	String			Web Mail	
log_subtype	N/A	log_subtype	String			Allowed Denied Pending	
severity	N/A	N/A	String				
user_name	Username	user	String	384	The end-user associated with the item being analysed		Web: End-user associated with the item being analysed Email: Recipient email address
src_ip	N/A	src_ip					
filename	File Name	file_name	String	1024	The original filename of the item being analysed		Web: This is the filename reported by the server in the `Content-disposition:` header of the HTTP response. If this header is not available, it will be the file part of the original URL Email: This is the file attachment with email (extracted from email MIME)
filetype	File Type	file_type	String	32	The MIME type of the file being analysed		Web: (? this is as reported by the source server in the `Content-type:` header of the HTTP response) Email: File type of file attachment
filesize	N/A	file_size	Number	int32	The size in bytes of the file being analysed		Web: This will usually differ from the bytes transferred in the corresponding HTTP transaction because it excludes HTTP headers and any compression used in transit.
file_hash	File Hash / Checksum	sha1sum	String	64	In 17.5 and earlier the sha1sum contained the sha1 checksum of the file being analyzed. In 18.0 and later the sha1sum contains the sha256 checksum of the file. In Central Reporting format this is called file_hash. The checksum is used to identify individual files and as the key when caching results. Although the checksum is not considered secure for data encryption purposes due to the risk of collision, it is sufficiently hard to deliberately generate files with checksum collisions that its use here is considered safe.		
source	Source	host	String	256	The origin of the item being analysed		Web: FQDN part of the URL (e.g. for content downloaded from http://fs1.cdn.example.com/files/example.exe, this will say "fs1.cdn.example.com") Email: Sender email address

reason	Reason	reason	String	256	A text description of the reason or event that triggered the log line	eligible pending cached clean cached malicious cloud clean cloud malicious error	`eligible`: Records the fact that a file was identified by the local scan engine as requiring analysis by Sandstorm. These log lines are intended only as a way of counting eligible items for reporting purposes, so the detail fields are left blank. `pending`: Records the fact that a file required further analysis. The file will be queued for sending to Sandstorm and the end-user will be notified that the scan is in progress `cached clean`: The file has been previously analysed and is known to be clean. `cached malicious`: The file has been previously analysed and is known to be malicious. `cloud clean`: A result was returned from the Sandstorm service after analysis indicating that the file is considered clean. `cloud malicious`: A result was returned from the Sandstorm service after analysis indicating that the file is considered malicious. `error`: An error occurred in processing the item. This includes failures to communicate with the Sandstorm service, errors reported by the Sandstorm service and internal errors such as problems with storage of items being scanned
destination	domain	domain	String	256	The destination domain of the email		Only applies to emails scanned by Sandstorm.
subject	subject	subject	String	64	The subject of the email		Only applies to emails scanned by Sandstorm.
log_id		N/A	String				eg. "010101600001"
device_name		N/A	String				eg "SFW"
device_model		N/A	String				eg "SF01V"
device_serial_id		N/A	String				eg "SFDemo-ff94e90"
user_group		N/A	String				eg. "student"
src_country		N/A	String		ISO 3166 (A 3) Code		eg. "IND"
dst_country		N/A	String		ISO 3166 (A 3) Code		eg. "USA"
src_port		N/A	Number				eg. 57067
dst_port		N/A	Number				eg. 20480
dst_ip		N/A	INET		IPv4,IPv6		eg. "20.20.20.20"

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `sandbox_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Sandbox	
log_component	Log Comp	log_component	String			Web Mail	
log_subtype	N/A	log_subtype	String			Allowed Denied Pending	
priority	N/A	N/A	String				
user_name	Username	user	String	384	The end-user associated with the item being analysed		Web: End-user associated with the item being analysed Email: Recipient email address
src_ip	N/A	src_ip					

filename	File Name	file_name	String	1024	The original filename of the item being analysed		Web: This is the filename reported by the server in the `Content-disposition:` header of the HTTP response. If this header is not available, it will be the file part of the original URL Email: This is the file attachment with email (extracted from email MIME)
filetype	File Type	file_type	String	32	The MIME type of the file being analysed		Web: (? this is as reported by the source server in the `Content-type:` header of the HTTP response) Email: File type of file attachment
filesize	N/A	file_size	Number	int32	The size in bytes of the file being analysed		Web: This will usually differ from the bytes transferred in the corresponding HTTP transaction because it excludes HTTP headers and any compression used in transit.
sha1sum	File Hash / Checksum	sha1sum	String	64	In 17.5 and earlier the sha1sum contained the sha1 checksum of the file being analyzed. In 18.0 and later the sha1sum contains the sha256 checksum of the file. The checksum is used to identify individual files and as the key when caching results. Although the checksum is not considered secure for data encryption purposes due to the risk of collision, it is sufficiently hard to deliberately generate files with checksum collisions that its use here is considered safe.		
source	Source	host	String	256	The origin of the item being analysed		Web: FQDN part of the URL (e.g. for content downloaded from http://fs1.cdn.example.com/files/example.exe, this will say "fs1.cdn.example.com") Email: Sender email address
reason	Reason	reason	String	256	A text description of the reason or event that triggered the log line	eligible pending cached clean cached malicious cloud clean cloud malicious error	`eligible`: Records the fact that a file was identified by the local scan engine as requiring analysis by Sandstorm. These log lines are intended only as a way of counting eligible items for reporting purposes, so the detail fields are left blank. `pending`: Records the fact that a file required further analysis. The file will be queued for sending to Sandstorm and the end-user will be notified that the scan is in progress `cached clean`: The file has been previously analysed and is known to be clean. `cached malicious`: The file has been previously analysed and is known to be malicious. `cloud clean`: A result was returned from the Sandstorm service after analysis indicating that the file is considered clean. `cloud malicious`: A result was returned from the Sandstorm service after analysis indicating that the file is considered malicious. `error`: An error occurred in processing the item. This includes failures to communicate with the Sandstorm service, errors reported by the Sandstorm service and internal errors such as problems with storage of items being scanned
destination	domain	domain	String	256	The destination domain of the email		Only applies to emails scanned by Sandstorm.
subject	subject	subject	String	64	The subject of the email		Only applies to emails scanned by Sandstorm.
log_id		N/A	String				eg. "010101600001"
device		N/A	String				eg "SFW"
device_name		N/A	String				eg "SF01V"
device_id		N/A	String				eg "SFDemo-ff94e90"

Sample logs

Message ID	Log
18041	device="SFW" date=2016-12-02 time=18:27:55 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=136501618041 log_type="Sandbox" log_component="Web" log_subtype="Allowed" priority=Information user_name="" src_ip= filename="" filetype="" filesize=0 sha1sum="" source="" reason="eligible" destination="" subject="" device="SFW" date=2016-12-02 time=18:31:50 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=136501618041 log_type="Sandbox" log_component="Web" log_subtype="Allowed" priority=Information user_name="rich" src_ip=192.168.73.220 filename="test7.exe" filetype="application/octet-stream" filesize=871700 sha1sum="7769b038037bc8e5c6373e92f99aa2324eee827c" source="floater.baldrys.ca" reason="cloud clean" destination="" subject=""
18042	device="SFW" date=2018-06-21 time=23:43:25 timezone="CEST" device_name="SG650" device_id=SFDemo-058196d log_id=136502218042 log_type="Sandbox" log_component="Web" log_subtype="Denied" priority=Critical user_name="ta-client" src_ip=10.146.13.251 filename="sandbox_dirty_no_cache" filetype="text/plain" filesize=266541 sha1sum="dd0bf29e56e4433e7dcffbe35f4003b1f251ce9d" source="ta-web-static.qa.astaro.de" reason="cached malicious" destination="" subject=""
18043	device="SFW" date=2016-12-02 time=18:27:55 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=136528618043 log_type="Sandbox" log_component="Web" log_subtype="Pending" priority=Information user_name="rich" src_ip=192.168.73.220 filename="badb.exe" filetype="application/octet-stream" filesize=1634319 sha1sum="9379f98b00017db44f3c6120bde7bdcd680296cb" source="floater.baldrys.ca" reason="pending" destination="" subject=""

Reporting

- Reports under:
  - Sandstorm: Reports > Network & Threats > Sandstorm
- Log identifier for reports:
  - Sandstorm: Log Type = Sandbox & Log Component = (Web or Mail) & Log Subtype = (Allowed or Denied or Pending)

SD-WAN

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_sdwan_GWnRT_log_fmt`.

Syslog Field Name	Log Viewer	Data Type	Length	Format /Description	Possible Values	Notes / Example
timestamp	N/A	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	N/A	String				SFW
device_model	N/A	String				SF01V
device_serial_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"
log_type	log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	log_component	String			Profile	eg. log_component="Profile"
log_subtype	log_subtype	String			Health check Route change	eg. log_subtype="Health check"
log_version	N/A	Number			1	eg. log_version=1
severity	severity	String			Notice	eg. severity="Notice"
status	status	String			Available Unavailable	eg. status="Available"
profile_id	profile_id	Number				eg. profile_id=123
profile_name	profile_name	String				eg. profile_name="test_profile"
gw_id	gw_id	Number				eg. gw_id=2
gw_name	gw_name	String				eg. gw_name="gw1"

message	message	String			• Gateway ***<name> (<IP address>)*** available. < probe protocol TCP probe/Ping> to ***<destination IP>*** successful. • Gateway ***<name> (<IP address>)*** unavailable. <probe protocol TCP probe/Ping> to ***<destination IP>*** failed. • Gateway ***<name> (<IP address>)*** unavailable. <probe protocol TCP probe/Ping> to ***<destination IP>, <destination IP>*** failed. • SD-WAN route changed for SD-WAN profile <name> from gateway <name> (<IP address>) to <name> (<IP address>	eg. message="Gateway ***gw1 (10.20.30.40)*** available. probe protocol TCP probe to ***10.20.30.50*** successful."
probe_target	probe_target	String			<IP Address>	probe_target="1.2.3.4, 5.6.7.8"
protocol	protocol	String			PING/TCP	protocol="PING"

Sample logs

Message ID	Logs
19021	`Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="158739519021" log_type="SD-WAN" log_component="Profile" log_subtype="Health check" log_version=1 severity="Notification" status="Available" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="Gateway gw1 (10.20.30.40) available. probe protocol TCP probe to 10.20.30.50 successful" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`
19022	`Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="158739519022" log_type="SD-WAN" log_component="Profile" log_subtype="Health check" log_version=1 severity="Notification" status="Unavailable" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="Gateway gw1 (10.20.30.40) unavailable. probe protocol TCP probe to 10.20.30.50, 10.20.30.60 failed" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`
19026	`Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="158940519026" log_type="SD-WAN" log_component="Route" log_subtype="Route change" log_version=1 severity="Notification" status="" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="SD-WAN route changed for SD-WAN profile test_profile1 from gateway gw2 (20.30.40.50) to gw1 (10.20.30.40)"`

Log format name under crformatter.conf is *CR_sdwan_SLA_met_log_fmt*.

Syslog Field Name	Log Viewer	Data Type	Length	Format /Description	Possible Values	Notes / Example
timestamp	N/A	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"

device_name	N/A	String				SFW
device_model	N/A	String				SF01V
device_serial_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"
log_type	log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	log_component	String			Profile	eg. log_component="Profile"
log_subtype	log_subtype	String			Health check	eg. log_subtype="Health check"
log_version	N/A	Number			1	eg. log_version=1
severity	severity	String			Notice	eg. severity="Notice"
status	status	String			SLA met SLA not met	eg. status="SLA met"
profile_id	profile_id	Number				eg. profile_id=123
profile_name	profile_name	String				eg. profile_name="test_profile"
gw_id	gw_id	Number				eg. gw_id=2
gw_name	gw_name	String				eg. gw_name="gw1"
latency	latency	Number			-1 if packet_loss is 100%	eg. latency=123
jitter	jitter	Number			-1 if packet_loss is 100%	eg. jitter=123
packet_loss	packet_loss	Number				eg. packet_loss=123
message	message	String			• SLA met for gateway ***<name> (<IP address>)*** using probe target ***<IP address>***. • SLA not met for gateway ***<name> (<IP address>)*** using probe target ***<IP address>***.	eg. message="SLA met for gateway gw1 (10.20.30.40) using probe target 10.20.30.50"
probe_target	probe_target	String			<IP Address>	probe_target="1.2.3.4, 5.6.7.8"
protocol	protocol	String			PING/TCP	protocol="PING"

Sample logs

Message ID	Logs
19023	`Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="158739519023" log_type="SD-WAN" log_component="Profile" log_subtype="Health check" log_version=1 severity="Notification" status="SLA met" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" latency=20 jitter=30 packet_loss=40 message="SLA met for gateway gw1 (10.20.30.40) using probe target 10.20.30.50" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`
19024	`Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="158739519024" log_type="SD-WAN" log_component="Profile" log_subtype="Health check" log_version=1 severity="Notification" status="SLA not met" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" latency=20 jitter=30 packet_loss=40 message="SLA not met for gateway gw2 (<20.30.40.50>) using probe target 10.20.30.50" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`

Log format name under crformatter.conf is `CR_sdwan_SLA_data_log_fmt`.

Syslog Field Name	Data Type	Length	Format /Description	Possible Values	Notes / Example
timestamp	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	String				SFW
device_model	String				SF01V
device_serial_id	String				SFDemo-ff87495
log_id	String				eg. log_id="010101600001"
log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	String			SLA	eg. log_component="SLA"
log_subtype	String			Information	eg. log_subtype="Information"
log_version	Number			1	eg. log_version=1
severity	String			Information	eg. severity="Information"
profile_id	Number				eg. profile_id=123
profile_name	String				eg. profile_name="test_profile"
gw_id	Number				eg. gw_id=2
gw_name	String				eg. gw_name="gw1"
latency	Number			-1 if packet_loss is 100%	eg. latency=123
jitter	Number			-1 if packet_loss is 100%	eg. jitter=123
packet_loss	Number				eg. packet_loss=123
start	Timestamp		ISO 8601		eg. start="2018-12-07T10:03:48+0000"
end	Timestamp		ISO 8601		eg. end="2018-12-07T10:03:48+0000"
gw_status	String			up/down	eg. gw_status="up"
sla_status	String			"SLA met"/"SLA not met"	eg. sla_status="SLA met"

Sample logs

Message ID	Logs
19025	`Dec 08 10:13:42 10.146.6.96 device_name="SFW" timestamp="2021-12-08T10:13:42-0500" device_model="SF01V" device_serial_id="SFDemo-c07-gulzar-vm-07" log_id=158825619025 log_type="SD-WAN" log_component="SLA" log_subtype="Information" log_version=1 severity="Information" profile_id=1 profile_name="test_profile" gw_id=3 gw_name="gw3" latency=11 start="2021-12-08T10:08:42-0500" end="2021-12-08T10:13:42-0500" gw_status="up" sla_status="SLA met"'`

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `sdwan_GWnRT_log_fmt`.

Syslog Field Name	Log Viewer	Data Type	Length	Format /Description	Possible Values	Notes / Example
device	N/A	String				SFW
device_name	N/A	String				SF01V
device_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"

log_type	log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	log_component	String			Profile	eg. log_component="Profile"
log_subtype	log_subtype	String			Health check Route change	eg. log_subtype="Health check"
priority	priority	String			Notice	eg. priority="Notice"
status	status	String			Available Unavailable	eg. status="Available"
profile_id	profile_id	Number				eg. profile_id=123
profile_name	profile_name	String				eg. profile_name="test_profile"
gw_id	gw_id	Number				eg. gw_id=2
gw_name	gw_name	String				eg. gw_name="gw1"
message	message	String			• Gateway ***<name> (<IP address>)*** available. < probe protocol TCP probe/Ping> to ***<destination IP>*** successful. • Gateway ***<name> (<IP address>)*** unavailable. <probe protocol TCP probe/Ping> to ***<destination IP>*** failed. • Gateway ***<name> (<IP address>)*** unavailable. <probe protocol TCP probe/Ping> to ***<destination IP>, <destination IP>*** failed. • SD-WAN route changed for SD-WAN profile <name> from gateway <name> (<IP address>) to <name> (<IP address>	eg. message="Gateway ***gw1 (10.20.30.40)*** available. probe protocol TCP probe to ***10.20.30.50*** successful."
probe_target	probe_target	String			<IP Address>	probe_target="1.2.3.4, 5.6.7.8"
protocol	protocol	String			PING/TCP	protocol="PING"

Sample logs

Message ID	Logs
19021	`device="SFW" date=2021-04-12 time=17:25:00 timezone="GMT" device_name="SFVUNL" device_id=SFDemo-qa-vm-246 log_id=158739519021 log_type="SD-WAN" log_component="Profile" log_subtype="Health check" priority=Notification status="Available" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="Gateway gw1 (10.20.30.40) available. probe protocol TCP probe to 10.20.30.50 successful" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`

19022	`device="SFW" date=2021-04-12 time=17:25:00 timezone="GMT" device_name="SFVUNL" device_id=SFDemo-qa-vm-246 log_id=158739519022 log_type="SD-WAN" log_component="Profile" log_subtype="Health check" priority=Notification status="Unavailable" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="Gateway gw1 (10.20.30.40) unavailable. probe protocol TCP probe to 10.20.30.50, 10.20.30.60 failed" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"`
19026	`device="SFW" date=2021-04-12 time=17:25:00 timezone="GMT" device_name="SFVUNL" device_id=SFDemo-qa-vm-246 log_id=158940519026 log_type="SD-WAN" log_component="Route" log_subtype="Route change" priority=Notification status="" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" message="SD-WAN route changed for SD-WAN profile test_profile1 from gateway gw2 (20.30.40.50) to gw1 (10.20.30.40)"`

Log format name under crformatter.conf is `sdwan_SLA_met_log_fmt`.

Syslog Field Name	Log Viewer	Data Type	Length	Format /Description	Possible Values	Notes / Example
device	N/A	String				SFW
device_name	N/A	String				SF01V
device_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"
log_type	log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	log_component	String			Profile	eg. log_component="Profile"
log_subtype	log_subtype	String			Health check	eg. log_subtype="Health check"
priority	priority	String			Notice	eg. priority="Notice"
status	status	String			SLA met SLA not met	eg. status="SLA met"
profile_id	profile_id	Number				eg. profile_id=123
profile_name	profile_name	String				eg. profile_name="test_profile"
gw_id	gw_id	Number				eg. gw_id=2
gw_name	gw_name	String				eg. gw_name="gw1"
latency	latency	Number			-1 if packet_loss is 100%	eg. latency=123
jitter	jitter	Number			-1 if packet_loss is 100%	eg. jitter=123
packet_loss	packet_loss	Number				eg. packet_loss=123
message	message	String			• SLA met for gateway ***<name> (<IP address>)*** using probe target ***<IP address>***. • SLA not met for gateway ***<name> (<IP address>)*** using probe target ***<IP address>***.	eg. message="SLA met for gateway gw1 (10.20.30.40) using probe target 10.20.30.50"
probe_target	probe_target	String			<IP Address>	probe_target="1.2.3.4, 5.6.7.8"
protocol	protocol	String			PING/TCP	protocol="PING"

Sample logs

Message ID	Logs

19023	device="SFW" date=2021-04-12 time=17:25:00 timezone="GMT" device_name="SFVUNL" device_id=SFDemo-qa-vm-246 log_id=158739519023 log_type="SD-WAN" log_component="Profile" log_subtype="Health check" priority=Notification status="SLA met" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" latency=20 jitter=30 packet_loss=40 message="SLA met for gateway gw1 (10.20.30.40) using probe target 10.20.30.50" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"
19024	device="SFW" date=2021-04-12 time=17:25:00 timezone="GMT" device_name="SFVUNL" device_id=SFDemo-qa-vm-246 log_id=158739519024 log_type="SD-WAN" log_component="Profile" log_subtype="Health check" priority=Notification status="SLA not met" profile_id=2 profile_name="test_profile" gw_id=4 gw_name="gw1" latency=20 jitter=30 packet_loss=40 message="SLA not met for gateway gw2 (<20.30.40.50>) using probe target 10.20.30.50" probe_target="10.20.20.25, 10.212.212.5" protocol="tcp"

Log format name under crformatter.conf is `sdwan_SLA_data_log_fmt`.

Syslog Field Name	Data Type	Length	Format /Description	Possible Values	Notes / Example
device	String				SFW
device_name	String				SF01V
device_id	String				SFDemo-ff87495
log_id	String				eg. log_id="010101600001"
log_type	String			SD-WAN	eg. log_type="SD-WAN"
log_component	String			SLA	eg. log_component="SLA"
log_subtype	String			Information	eg. log_subtype="Information"
priority	String			Information	eg. priority="Information"
profile_id	Number				eg. profile_id=123
profile_name	String				eg. profile_name="test_profile"
gw_id	Number				eg. gw_id=2
gw_name	String				eg. gw_name="gw1"
latency	Number			-1 if packet_loss is 100%	eg. latency=123
jitter	Number			-1 if packet_loss is 100%	eg. jitter=123
packet_loss	Number				eg. packet_loss=123
starttime	Timestamp				eg. starttime=12345
timestamp	Timestamp				eg. timestamp=1234567
gw_status	String			up/down	eg. gw_status="up"
sla_status	String			"SLA met"/"SLA not met"	eg. sla_status="SLA met"

Sample logs

Message ID	Logs
19025	device="SFW" date=2021-12-08 time=10:13:42 timezone="EST" device_name="SF01V" device_id=SFDemo-c07-gulzar-vm-07 log_id=158825619025 log_type="SD-WAN" log_component="SLA" log_subtype="Information" priority=Information profile_id=1 profile_name="test_profile" gw_id=3 gw_name="gw3" latency=11 jitter=0 packet_loss=0 starttime=1638976122 timestamp=1638976422 gw_status="up" sla_status="SLA met"

SSL/TLS Filter (Inspection)

Reporting

- CFR Reports under:
  - Log Viewer & Search
- SF On Box Reports under:
  - N/A
- Control Center:
  - SSL/TLS
- Log identifier for reports:
  - Log Type = SSL

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_tls_log_fmt`.

Syslog Field Name	Log Viewer	Data Type	Length	Format /Description	Possible Values	Notes / Example
timestamp	N/A	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device_name	N/A	String				SFW
device_model	N/A	String				SF01V
device_serial_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"
log_type	log_type	String			SSL	eg. log_type="SSL"
log_component	log_component	String			SSL	eg. log_component="SSL"
log_subtype	log_subtype	String			Decrypt Reject Reject and notify Do not decrypt Error	eg. log_subtype="Decrypt"
log_version	N/A	Number			1	eg. log_version=1
severity	severity	String			Information	eg. severity="Information"
user_name	user	String				eg. user_name="gaurav"
user_group	user_group	String				eg. user_group="student"
src_ip	src_ip	INET		IPv4,IPv6		eg. src_ip="10.10.10.10"
src_country	src_country	String		ISO 3166 (A 3) Code		eg. src_country="IND"
src_port	src_port	Number				eg. src_port=514
dst_ip	dst_ip	INET		IPv4,IPv6		eg. dst_ip="20.20.20.20"
dst_country	dst_country	String		ISO 3166 (A 3) Code		eg. dst_country="USA"
dst_port	dst_port	Number				eg. dst_port=514
src_zone_type	N/A	String				eg. src_zone_type="LAN"
src_zone	N/A	String				eg. src_zone="LAN"
dst_zone_type	N/A	String				eg. dst_zone_type="WAN"
dst_zone	N/A	String				eg. dst_zone="WAN"
app_name	app_name	String				eg. app_name="Skype"

con_id	con_id	String				eg. con_id=1084482152
rule_id	rule_id	Number				eg. rule_id=11
profile_id	profile_id	Number				eg. profile_id=8448215
bitmask	bitmask	String				eg. bitmask="xxx"
key_type	key_type	String				eg. key_type="RSA"
resumed	resumed	Number				
cert_chain_served	cert_chain_served	String				eg. cert_chain_served="xxx"
key_param	key_param	String				eg. key_param="xxx"
fingerprint	fingerprint	String				eg. fingerprint="d4:1d:8c:d9:8f:00:b2:04:e9:80:09:98:ec:f8:42:7e"
cipher_suite	cipher_suite	String				eg. cipher_suite="TLS"
sni	sni	String				eg. sni="HTTPS"
rule_name	rule_name	String				eg. rule_name="Network"
profile_name	profile_name	String				eg. profile_name="xxx"
tls_version	tls_version	String				eg. tls_version="xxx"
reason	reason	String				eg. reason="eligible"
exceptions	exception	String				eg. exceptions="av"
category	category	String				e.g. "Information Technology"

Sample logs

Message ID	Logs
19004	Apr 17 23:39:44 10.146.13.50 device_name="SFW" timestamp="2020-04-17T23:39:43+0200" device_model="SF01V" device_serial_id="SFDemo-ffe2599" log_id="148531619004" log_type="SSL" log_component="SSL" log_subtype="Decrypt" log_version=1 severity="Information" src_ip="10.146.6.42" dst_ip="10.8.142.181" src_country="R1" dst_country="R1" src_port=33962 dst_port=443 con_id="2128354112" rule_id=2 profile_id=1 rule_name="TA: Decrypt All" profile_name="Maximum compatibility" key_type="KEY_TYPE__RSA" fingerprint="c0:78:6d:b9:58:4d:f3:31:50:42:d8:b2:14:43:ff:be:d8:69:8a:4e" cert_chain_served="FALSE" cipher_suite="TLS_RSA_WITH_AES_128_CBC_SHA256" sni="www.apache.org" tls_version="TLS1.2" src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="Information Technology"
19005	Apr 18 01:12:33 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:12:33+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="148532619005" log_type="SSL" log_component="SSL" log_subtype="Reject" log_version=1 severity="Information" src_ip="10.146.13.238" dst_ip="10.8.142.181" src_country="R1" dst_country="R1" src_port=56834 dst_port=443 con_id="3017970624" rule_id=3 profile_id=1 rule_name="TA: Max Compatibility" profile_name="Maximum compatibility" key_type="KEY_TYPE__RSA" fingerprint="c0:78:6d:b9:58:4d:f3:31:50:42:d8:b2:14:43:ff:be:d8:69:8a:4e" cert_chain_served="FALSE" cipher_suite="TLS_RSA_WITH_AES_128_CBC_SHA256" sni="mozilla.com" tls_version="TLS1.2" reason="Blocked due to web policy" src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="Information Technology"
19006	Apr 18 02:07:28 10.146.6.128 device_name="SFW" timestamp="2020-04-18T02:07:27+0200" device_model="SF01V" device_serial_id="SFDemo-ff99653" log_id="148535619006" log_type="SSL" log_component="SSL" log_subtype="Error" log_version=1 severity="Information" src_ip="10.146.13.255" dst_ip="10.146.29.83" src_country="R1" dst_country="R1" src_port=34594 dst_port=443 con_id="353581568" rule_id=2 profile_id=4 rule_name="TA Inspection Rule" profile_name="TA_DECRYPTION_PROFILE" bitmask="Invalid issuer" key_type="KEY_TYPE__RSA" fingerprint="72:b4:7a:e2:e8:c4:27:46:92:26:53:71:3a:f9:df:76:14:45:88:c8" resumed=1 cert_chain_served="FALSE" cipher_suite="TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" sni="10.146.29.83" tls_version="TLS1.2" reason="Dropped due to TLS engine error: INCOMPLETE_SESS_DATA[1]" src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="IPAddress"
19007	
19008	

19009	
19011	
19012	Apr 18 01:13:48 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:13:48+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="148532619012" log_type="SSL" log_component="SSL" log_subtype="Reject" log_version=1 severity="Information" src_ip="10.146.13.238" dst_ip="10.8.142.181" src_country="R1" dst_country="R1" src_port=56840 dst_port=443 con_id="1127601088" rule_id=4 profile_id=5 rule_name="TA: block" profile_name="BlockUsingTlsVersion" key_type="KEY_TYPE__RSA" fingerprint="c0:78:6d:b9:58:4d:f3:31:50:42:d8:b2:14:43:ff:be:d8:69:8a:4e" cert_chain_served="FALSE" cipher_suite="TLS_RSA_WITH_AES_128_CBC_SHA256" sni="skizzenbuch.thalia.de" tls_version="TLS1.2" reason="Blocked due to TLS protocol version" src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="Online Shopping"
19013	
19014	
19015	
19016	Apr 18 01:10:25 10.146.6.96 device_name="SFW" timestamp="2020-04-18T01:10:25+0200" device_model="SF01V" device_serial_id="SFDemo-ffef173" log_id="148504619016" log_type="SSL" log_component="SSL" log_subtype="Drop" log_version=1 severity="Information" src_ip="10.146.13.238" dst_ip="13.35.253.122" src_country="R1" dst_country="USA" src_port=36972 dst_port=443 con_id="1460178048" rule_id=2 profile_id=4 rule_name="TA: TestTLSInspectionRule" profile_name="TestProfile" bitmask="Valid" key_type="KEY_TYPE__RSA" fingerprint="f8:7a:da:47:5a:11:e3:91:89:c2:10:66:79:39:9d:f9:c8:a2:67:44" cert_chain_served="TRUE" cipher_suite="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256" sni="sophostest.com" tls_version="TLS1.2" reason="Blocked due to exceeded decryption capability" src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="Information Technology"
19017	
19018	Apr 18 00:22:18 10.146.13.50 device_name="SFW" timestamp="2020-04-18T00:22:18+0200" device_model="SF01V" device_serial_id="SFDemo-ffe2599" log_id="148535619018" log_type="SSL" log_component="SSL" log_subtype="Error" log_version=1 severity="Information" src_ip="10.146.6.42" dst_ip="91.189.95.15" src_country="R1" dst_country="GBR" src_port=45272 dst_port=443 con_id="1488327616" rule_id=2 profile_id=1 rule_name="TA: Decrypt All" profile_name="Maximum compatibility" bitmask="Valid" key_type="KEY_TYPE__RSA" fingerprint="c4:0f:35:52:2f:c9:91:20:f5:8f:e2:c8:08:7f:ef:95:a9:e8:8a:fc" cert_chain_served="TRUE" cipher_suite="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" sni="changelogs.ubuntu.com" tls_version="TLS1.2" reason="TLS handshake fatal alert: unknown CA(48)." src_zone_type="LAN" src_zone="LAN" dst_zone_type="WAN" dst_zone="WAN" category="Information Technology"
19019	
19020	

Device Standard Format (Legacy)

Field descriptions

Log format name under crformatter.conf is `tls_log_fmt`.

Syslog Field Name	Log Viewer	Data Type	Length	Format/Description	Possible Values	Notes / Example
timestamp	N/A	Timestamp		ISO 8601		eg. timestamp="2018-12-07T10:03:48+0000"
device	N/A	String				SFW
device_name	N/A	String				SF01V
device_id	N/A	String				SFDemo-ff87495
log_id	N/A	String				eg. log_id="010101600001"
log_type	log_type	String			SSL	eg. log_type="SSL"
log_component	log_component	String			SSL	eg. log_component="SSL"

log_subtype	log_subtype	String			Decrypt Reject Reject and notify Do not decrypt Error	eg. log_subtype="Decrypt"
severity	severity	String			Information	eg. severity="Information"
user_name	user	String				eg. user_name="gaurav"
user_gp	user_group	String				eg. user_gp="student"
src_ip	src_ip	INET		IPv4,IPv6		eg. src_ip="10.10.10.10"
src_country	src_country	String		ISO 3166 (A 3) Code		eg. src_country="IND"
src_port	src_port	Number				eg. src_port=514
dst_ip	dst_ip	INET		IPv4,IPv6		eg. dst_ip="20.20.20.20"
dst_country	dst_country	String		ISO 3166 (A 3) Code		eg. dst_country="USA"
dst_port	dst_port	Number				eg. dst_port=514
app_name	app_name	String				eg. app_name="Skype"
con_id	con_id	String				eg. con_id=1084482152
rule_id	rule_id	Number				eg. rule_id=11
profile_id	profile_id	Number				eg. profile_id=8448215
bitmask	bitmask	String				eg. bitmask="xxx"
key_type	key_type	String				eg. key_type="RSA"
resumed	resumed	Number				
cert_chain_served	cert_chain_served	String				eg. cert_chain_served="xxx"
key_param	key_param	String				eg. key_param="xxx"
fingerprint	fingerprint	String				eg. fingerprint="d4:1d:8c:d9:8f:00:b2:04:e9:80:09:98:ec:f8:42:7e"
cipher_suite	cipher_suite	String				eg. cipher_suite="TLS"
sni	sni	String				eg. sni="HTTPS"
rule_name	rule_name	String				eg. rule_name="Network"
profile_name	profile_name	String				eg. profile_name="xxx"
tls_version	tls_version	String				eg. tls_version="xxx"
reason	reason	String				eg. reason="eligible"
exceptions	exception	String				eg. exceptions="av"
category	category	String				e.g. "Information Technology"
connectionname	N/A	String				
message	message	String				

SSL VPN

Log format name under crformatter.conf is `sslvpn_log_fmt`.

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type	log_type	String			Event	
log_component	log_component	String			SSL VPN	
log_subtype	log_subtype	String			System	
priority		String			Information	
mode	access_type	String		The type of connection.	"Site to Site" "Remote Access"	
starttime	start_time			Time of the beginning of the connection	1489578289	
user_name	user	String	384		"-" in case of mode "Site to Site" "someusername" else	
ipaddress	src_ip			ip address of our side	e.g. "10.81.234.5"	
sent_bytes	bytes_sent	Number	int32	Number of bytes sent		
recv_bytes	bytes_received	Number	int32	Number of bytes received		
status	status	String			"Established" "Terminated"	
message	message	String	1024	Message describing the current event	""SSL VPN Site to site connection '%s' established" "SSL VPN User '%s' connected " "SSL VPN Site to site connection '%s' disconnected" "SSL VPN User '%s' disconnected"	
timestamp	event_timestamp					
connectionname	con_name	String	384			
remote_ip	dst_ip			ip address of other side	e.g. "10.81.234.5"	

Reporting

- Reports under:
  - SSL VPN: Reports > VPN > SSL VPN
  - Also use to report:
    - Reports > Compliance > Events > System Events
- Log identifier for reports:
  - SSL VPN: Log Type = Event & Log Subtype = System & Log Component = SSL VPN

Sample logs

Message ID	Log

17824	device="SFW" date=2017-03-15 time=17:14:53 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062811617824 log_type="Event" log_component="SSL VPN" log_subtype="System" priority=Information Mode="Site to Site" sessionid= starttime=0 user_name="-" ipaddress=10.81.234.5 sent_bytes=0 recv_bytes=0 status="Established" message="SSL VPN Site to site connection 'GauravPatel235' established" timestamp=1489578293 connectionname="GauravPatel235" remote_ip=10.81.234.6
17825	device="SFW" date=2017-03-15 time=17:16:01 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062811617825 log_type="Event" log_component="SSL VPN" log_subtype="System" priority=Information Mode="Site to Site" sessionid= Reason="Logout" starttime=1489578289 user_name="-" ipaddress=10.81.234.5 sent_bytes=5719 recv_bytes=5435 status="Terminated" message="SSL VPN Site to site connection 'GauravPatel235' disconnected" timestamp=1489578361 connectionname="GauravPatel235" remote_ip=10.81.234.6

SSL VPN (resource)

Log format name under crformatter.conf is `sslvpn_tr_log_fmt`.

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	log_type	String			Event	
log_component	log_component	String			SSL VPN	
log_subtype	log_subtype	String			System	
priority		String				
Mode	access_type	String				
sessionid	session_id	String	64			
resource_type	protocol	String				
resource	url	String	256			
user_name	user	String	384			
ipaddress	src_ip					
message	message	String	1024			

Reporting

- Reports under:
  - SSL VPN: Reports > VPN > SSL VPN
  - Also use to report:
    - Reports > Compliance > Events > System Events
- Log identifier for reports:
  - SSL VPN: Log Type = Event & Log Subtype = System & Log Component = SSL VPN

Sample logs

Message ID	Log
17830	`device="SFW" date=2017-03-15 time=17:35:29 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062811617830 log_type="Event" log_component="SSL VPN" log_subtype="System" priority=Information Mode="Web Access" sessionid=mpvoi6p1ift85styukwck3ym resource_type="HTTPS" resource=" https://www.facebook.com" sslvpnpolicyname=GauravPatel user_name="gaurav" ipaddress=10.198.47.103 status="Allow" message="User gaurav was allowed access of the HTTPS resource https://www.facebook.com using Web Access"`  `device="SFW" date=2017-03-15 time=17:35:29 timezone="IST" device_name="CR750iNG-XP" device_id=C44313350024-P29PUA log_id=062811617830 log_type="Event" log_component="SSL VPN" log_subtype="System" priority=Information Mode="Web Access" sessionid=mpvoi6p1ift85styukwck3ym resource_type="HTTPS" resource=" https://www.facebook.com" sslvpnpolicyname=GauravPatel user_name="gaurav" ipaddress=10.198.47.103 status="Allow" message="User gaurav was allowed access of the HTTPS resource https://www.facebook.com using Web Access"`
17831	

System health (events)

Log format name under crformatter.conf is `sysh_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type		log_type	String			System Health	
log_component		log_component	String			CPU Memory Disk Live User Interface	
log_subtype		log_subtype	String			Usage	
priority			String				
raw_data					This is not the field but combination of multiple fields.		

Reporting

- Not capture for Reporting (Logs use to report SF Resource Usage on Sophos iView)
- Log identifier for reports:
  - System Health (Events): Log Type = System Health & Log Component = (CPU or Memory or Disk or Live User or Interface) & Log Subtype = Usage

Sample logs

Message ID	Log
18031	`device="SFW" date=2018-06-05 time=15:10:00 timezone="CEST" device_name="SF01V" device_id=SFDemo-fe75a9f log_id=127626618031 log_type="System Health" log_component="CPU" log_subtype="Usage" priority=Information system=1.29% user=7.60% idle=91.11%` `device="SFW" date=2018-06-05 time=15:10:00 timezone="CEST" device_name="SF01V" device_id=SFDemo-fe75a9f log_id=127726618031 log_type="System Health" log_component="Memory" log_subtype="Usage" priority=Information unit=byte total_memory=2100191232 free=578650112 used=1521541120` `device="SFW" date=2018-06-05 time=15:10:00 timezone="CEST" device_name="SF01V" device_id=SFDemo-fe75a9f log_id=123526618031 log_type="System Health" log_component="Interface" log_subtype="Usage" priority=Information interface=Port1 receivedkbits=4.55 transmittedkbits=2.03 receivederrors=0.00 transmitteddrops=0.00 collisions=0.00 transmittederrors=0.00 receiveddrops=0.00`  `device="SFW" date=2018-06-05 time=15:10:00 timezone="CEST" device_name="SF01V" device_id=SFDemo-fe75a9f log_id=127826618031 log_type="System Health" log_component="Disk" log_subtype="Usage" priority=Information Configuration=13.00% Reports=11.00% Signature=11.00% Temp=4.00%`  `device="SFW" date=2018-06-05 time=15:10:00 timezone="CEST" device_name="SF01V" device_id=SFDemo-fe75a9f log_id=127926618031 log_type="System Health" log_component="Live User" log_subtype="Usage" priority=Information users=0`

Version upgrade (events)

Log format name under crformatter.conf is `ver_update_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type		log_type	String			Event	
log_component		log_component	String			eDial-In Anti-Virus IPS WEBCAT HA ATP SSLVPN clients IPSEC clients Authentication clients RED Firmware AP Firmware Up2Date Web Application Firewall	
log_subtype		log_subtype	String			System	
priority			String			Notice Information	
message		message	String	1024			

Reporting

- Reports under:
  - Version Upgrade Event: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - Version Upgrade Event: Log Type = Event & Log Subtype = System

Sample logs

Message ID	Log
17821	`device="SFW" date=2018-06-05 time=03:36:30 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=064211617821 log_type="Event" log_component="Dial-In" log_subtype="System" priority=Information status="Successful" message="Dialin client connected"`
17822	`device="SFW" date=2018-06-05 time=03:36:30 timezone="BST" device_name="XG330" device_id=C310073TWB2Y249 log_id=064211617822 log_type="Event" log_component="Dial-In" log_subtype="System" priority=Information status="Successful" message="Dialin client Disconnected"`

17819	`messageid="17819" log_type="Event" log_component="Anti-Virus" log_subtype="System" status="Successful" additional_information="oldversion=1.0.23242 newversion=1.0.23243 " message="Avira AV definitions upgraded from 1.0.23242 to 1.0.23243."`
	
	`messageid="17819" log_type="Event" log_component="Anti-Virus" log_subtype="System" status="Successful" additional_information="oldversion=1.0.12667 newversion=1.0.12668 " message="Sophos AV definitions upgraded from 1.0.12667 to 1.0.12668."`

17818	device="SFW" date=2018-06-05 time=12:01:56 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=063911517818 log_type="Event" log_component="IPS" log_subtype="System" priority=Notice status="Successful" oldversion=3.12.36 newversion=3.14.85 message="IPS definitions upgraded from 3.12.36 to 3.14.85."
17817	This log is related to "WebCat Database upgraded from <old version> to <new version>"
17920	This log is related to "Auto-update of External URL Database for Web Category" / "WebCat database upgrade failed".
17921	device="SFW" date=2018-06-05 time=11:30:11 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=063911617921 log_type="Event" log_component="IPS" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade definitions for IPS"
17922	device="SFW" date=2018-06-05 time=11:30:40 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=064011617922 log_type="Event" log_component="Anti-Virus" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade definitions for SOPHOS AV"
17923	device="SFW" date=2018-06-05 time=13:00:02 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=063311617923 log_type="Event" log_component="Appliance" log_subtype="System" priority=Information backup_mode='appliance' message="Scheduled backup was successfully sent to appliance "
60012	device="SFW" date=2018-06-05 time=08:51:56 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611560012 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="Appliance with appliance key C30006CBC4838C2 becomes standalone"
60013	device="SFW" date=2018-06-05 time=12:56:37 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560013 log_type="Event" log _component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B goes in fault"
60014	device="SFW" date=2018-06-05 time=15:06:51 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560014 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B becomes auxiliary"
60015	device="SFW" date=2018-06-05 time=08:55:16 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611560015 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="Appliance with appliance key C30006CBC4838C2 becomes primary"
60016	device="SFW" date=2018-06-05 time=09:05:18 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560016 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B becomes standalone at appliance startup"
60017	device="SFW" date=2018-06-05 time=15:07:01 timezone="BST" device_name="XG310" device_id=C30006T22TGR89B log_id=061611560017 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006T22TGR89B message="Appliance with appliance key C30006T22TGR89B goes in fault at appliance startup"
60018	device="SFW" date=2018-06-05 time=09:09:08 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611560018 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="Appliance with appliance key C30006CBC4838C2 becomes auxiliary at appliance startup"
60019	device="SFW" date=2018-06-05 time=09:11:18 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611560019 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="Appliance with appliance key C30006CBC4838C2 becomes primary at appliance startup"
17838	device="SFW" date=2018-06-05 time=09:11:18 timezone="BST" device_name="XG310" device_id=C30006CBC4838C2 log_id=061611517838 log_type="Event" log_component="HA" log_subtype="System" priority=Notice status="Successful" Appliance_Key=C30006CBC4838C2 message="HA was disabled because firmware upgrade to auxiliary appliance with appliance key S210055D2BDFDDD failed. Firmware successfully upgraded on primary appliance with appliance key C30006CBC4838C2"

18017	device="SFW" date=2018-06-05 time=12:31:10 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=066911518017 log_type="Event" log_component="ATP" log_subtype="System" priority=Notice status="Successful" oldversion=1.0.001 newversion=1.0.0195 message="ATP definitions upgraded from 1.0.001 to 1.0.0195."
18018	device="SFW" date=2018-06-05 time=11:31:54 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=066911618018 log_type="Event" log_component="ATP" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade definitions for ATP"
18019	device="SFW" date=2018-06-05 time=12:01:57 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067011518019 log_type="Event" log_component="SSLVPN Client" log_subtype="System" priority=Notice status="Successful" oldversion=0 newversion=1.0.007 message="SSLVPN clients upgraded from 0 to 1.0.007."
18020	device="SFW" date=2018-06-05 time=11:32:26 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067011618020 log_type="Event" log_component="SSLVPN Client" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade SSLVPN clients"
18021	N/A. SFOS does not have IPsec clients. This message is for IPsec clients upgraded from old_version to new_version.
18022	N/A. SFOS does not have IPsec clients. This message is for Failed to upgrade IPsec clients.
18023	device="SFW" date=2018-06-05 time=12:13:32 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067211518023 log_type="Event" log_component="Authentication Client" log_subtype="System" priority=Notice status="Successful" oldversion=0 newversion=1.0.0011 message="Authentication clients upgraded from 0 to 1.0.0011."
18024	device="SFW" date=2018-06-05 time=11:33:12 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067211618024 log_type="Event" log_component="Authentication Client" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade Authentication clients"
18025	device="SFW" date=2018-06-05 time=12:32:32 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067311518025 log_type="Event" log_component="RED Firmware" log_subtype="System" priority=Notice status="Successful" oldversion=0 newversion=2.0.014 message="RED firmware upgraded from 0 to 2.0.014."
18026	device="SFW" date=2018-06-05 time=11:33:45 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067311618026 log_type="Event" log_component="RED Firmware" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade RED firmware"
18027	device="SFW" date=2018-06-05 time=11:45:49 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067411518027 log_type="Event" log_component="AP Firmware" log_subtype="System" priority=Notice status="Successful" oldversion=7.0.001 newversion=11.0.001 message="AP firmware upgraded from 7.0.001 to 11.0.001."
18028	device="SFW" date=2018-06-05 time=11:34:08 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067411618028 log_type="Event" log_component="AP Firmware" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade AP firmware"
18029	device="SFW" date=2018-06-05 time=11:17:58 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067511518029 log_type="Event" log_component="Up2Date" log_subtype="System" priority=Notice status="Failed" message="Failed to check for updates"
18030	device="SFW" date=2018-06-05 time=11:21:41 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=067511618030 log_type="Event" log_component="Up2Date" log_subtype="System" priority=Notice status="Failed" message="Failed to download file apfw_1.00_11.0.001.tar.gz.gpg"
18033	device="SFW" date=2018-06-05 time=12:00:30 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=065011518033 log_type="Event" log_component="Web Application Firewall" log_subtype="System" priority=Notice status="Successful" oldversion=1.0.001 newversion=1.0.0006 message="WAF rules upgraded from 1.0.001 to 1.0.0006."
18034	device="SFW" date=2018-06-05 time=11:28:34 timezone="BST" device_name="SG230" device_id=S2100561D01E28D log_id=065011618034 log_type="Event" log_component="Web Application Firewall" log_subtype="System" priority=Notice status="Failed" message="Failed to upgrade WAF rules"

WAF

Log format name under crformatter.conf is `waf_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	log_type	log_type	String		Log type	WAF	
log_component	log_component	log_component	String		Log component	Web Application Firewall	
priority	priority		String		Message priority		
user_name	user_name	user	String	384	the userid of the person requesting the document as determined by HTTP authentication.		If the status code for the request (see below) is 401, then this value should not be trusted because the user is not yet authenticated. If the document is not password protected, this part will be "-"
server	server	server	String	256	first domain name of the virtual server serving the request		
sourceip	Source IP	src_ip			IP address of client (or proxy) that initiates the request		
localip	Local IP	local_ip			IP address of used backend server. Might be "-" in case the request didn't cause a backend connection.		
ws_protocol	Websocket Protocol	protocol	String	16	marks the usage of Websocket protocol.		
url	url	url	String	1024	URL path requested, not including any query string		
queryString	Query String	query_string	String	1024	the query string (prepended with a ? if a query string exists, otherwise an empty string)		
cookie	cookie	cookie	String	4096	contents of Cookie: header line in the request sent by the reverse proxy to the server		
referer	referer	referer	String	1024	contents of Referer: header line in the request sent to the server		
method	method	method	String	16	the request method		GET, POST, etc. any request method allowed by the standard
httpstatus	HTTP status code	Status Code	Number	int16	HTTP status code	standard HTTP status codes	

reason	reason	Reason	String	32	reverse proxy feature that intercepted a request.	"waf" "cookie" "url hardening" "av" "geoip" "dnsrbl" "-"	If the request was intercepted this field will contain the WAF feature that intercepted the request. reason="waf" This reason is given for requests blocked due to a recognized SQL Injection Attack or a recognized XSS attack. reason="cookie" This reason is given for requests blocked due to unsigned or invalidly signed cookies (unless configured to drop such invalid cookies from the request, which is the default since ASG 8.200). reason="url hardening" This reason is given for requests blocked by URL Hardening due to a missing or invalid URL signature. reason="form hardening" This reason is given for requests blocked by Form Hardening due to recognized unauthorized form modifications. reason="av" This reason is given for requests blocked by the Anti Virus engine(s). reason="geoip" or reason="dnsrbl" This reason is given for requests blocked due to bad reputation of the client's IP address. The reason="geoip" indicates that this request was blocked due to the client's IP address being listed in the GeoIP database. The reason="dnsrbl" indicates that this request was blocked due to the client's IP address being listed in a DNS realtime blocking list (RBL). In case the request was not intercepted, this field contains the value "-".
extra	extra	Message	String	256	additional information on why a request was intercepted.		In case the request was not intercepted, this field contains the value "-".
contenttype	Content type	content_type	String	64	contents of Content-type: header line in the request sent to the server		
useragent	User agent	user_agent	String	256	contents of User-Agent: header line in the request sent to the server		
responsetime	Response time	response_time	Number	int32	time taken to serve the request, in microseconds		
bytessent	Bytes sent	bytes_sent	Number	int32	amount of bytes sent while serving the request		
bytesrcv	Bytes received	bytes_received	Number	int32	amount of bytes received while serving the request		
fw_rule_id	Firewall rule ID	fw_rule_id	Number	int32	The firewall ruleid the WAF rule is connected to.		

Reporting

- Reports under:
  - WAF Allowed: Reports > Applications & Web > Web Server Usage
  - WAF Denied: Reports > Applications & Web > Web Server Protection
- Log identifier for reports:
  - WAF Allowed: Log Type = WAF & Log Component = Web Application Firewall & Log Subtype = Allowed
  - WAF Denied: Log Type = WAF & Log Component = Web Application Firewall & Log Subtype = Denied

Sample logs

Message ID	Log
17071	`messageid="17071" log_type="WAF" log_component="Web Application Firewall" user="-" server="dev-mpetrenyi-02.qa.astaro.de" src_ip="10.69.96.94" local_ip="10.8.17.51" protocol="HTTP/1.1" url="/favicon.ico" query_string="" cookie="-" referer="-" method="GET" response_code="404" reason="-" extra="-" content_type="text/html" user_agent="Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" response_time="281" bytes_sent="411" bytes_received="258" fw_rule_id="2"`

Web (System HTTPS Deny events)

There are two log messages that can be triggered by the web proxy that appear in syslog under "System events" and in Log viewer under "System". In DPI mode the equivalent logs are part of SSL/TLS filter.

Central Reporting Format

Log format name under crformatter.conf is `CR_https_deny_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Event	
log_component	Log Comp	log_component	String			HTTPS	
log_subtype	N/A	log_subtype	String			System	
priority	N/A	N/A	String				
destination	N/A	dst_ip					
message	Message	message	String	1024			• Unknown protocol traffic is denied. Disable "Block unrecognized SSL protocols" option from "Web -> Protection - > HTTPS Decryption and Scanning" to access HTTPS site at '10.8.141.178' • HTTPS access is denied due to invalid server certificate. Disable "Block invalid certificates" from "Web -> Protection -> HTTPS Decryption and Scanning" to access HTTPS site 'https://expired.badssl.com/'
user_agent	N/A	user_agent	String	256			
status_code	N/A	status_code	Number	int16			
log_id		N/A	String				eg. "010101600001"
device_name		N/A	String				eg "SFW"
device_model		N/A	String				eg "SF01V"
device_serial_id		N/A	String				eg "SFDemo-ff94e90"
log_version		N/A	Number			1	eg. log_version=1
protocol	N/A	N/A	String		IP protocol used fro the connection	"TCP"	
src_ip	Source IP	N/A			The IP address from which the HTTP /HTTPS connection originated		
src_port	N/A	N/A			The port from which the HTTP/HTTPS connection originated		
src_country	source country	N/A	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"	
src_zone_type		N/A	String				eg. src_zone_type="LAN"
src_zone		N/A	String				eg. src_zone="LAN"
dst_port	N/A	N/A			The port to which the HTTP/HTTPS connection was made		
dst_country	destination country	N/A	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"	
dst_zone_type		N/A	String				eg. dst_zone_type="WAN"
dst_zone		N/A	String				eg. dst_zone="WAN"

Device Standard Format

Log format name under crformatter.conf is `https_deny_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format /Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Event	
log_component	Log Comp	log_component	String			HTTPS	
log_subtype	N/A	log_subtype	String			System	
priority	N/A	N/A	String				
destination	N/A	dst_ip					
message	Message	message	String	1024			• Unknown protocol traffic is denied. Disable "Block unrecognized SSL protocols" option from "Web -> Protection -> HTTPS Decryption and Scanning" to access HTTPS site at '10.8.141.178' • HTTPS access is denied due to invalid server certificate. Disable "Block invalid certificates" from "Web -> Protection -> HTTPS Decryption and Scanning" to access HTTPS site 'https://expired.badssl.com/'
user_agent	N/A	user_agent	String	256			
status_code	N/A	status_code	Number	int16			
log_id		N/A	String				eg. "010101600001"
device		N/A	String				eg "SFW"
device_name		N/A	String				eg "SF01V"
device_id		N/A	String				eg "SFDemo-ff94e90"

Sample logs

Message ID	Log
17916	`device="SFW" date=2018-06-21 time=21:15:03 timezone="CEST" device_name="SG650" device_id=SFDemo-bb7c726 log_id=064811517916 log_type="Event" log_component="HTTPS" log_subtype="System" priority=Notice destination=10.8.141.178 message="Unknown protocol traffic is denied. Disable "Block unrecognized SSL protocols" option from "Web -> Protection -> HTTPS Decryption and Scanning" to access HTTPS site at '10.8.141.178'#012" user_agent="" status_code=0`
17917	`device="SFW" date=2018-06-21 time=23:52:25 timezone="CEST" device_name="SF01V" device_id=SFDemo-814c0fd log_id=064811517917 log_type="Event" log_component="HTTPS" log_subtype="System" priority=Notice destination=104.154.89.105 message="HTTPS access is denied due to invalid server certificate. Disable "Block invalid certificates" from "Web -> Protection -> HTTPS Decryption and Scanning" to access HTTPS site 'https://self-signed.badssl.com/'#012" user_agent="" status_code=0`

Reporting

- Reports under:
  - HTTPS Deny Events: Reports > Compliance > Events > System Events
- Log identifier for reports:
  - HTTPS Deny Events: Log Type = Event & Log Subtype = System & Log Component = HTTPS

Web content policy

Web content policy transactions are generally logged with `log_type="Content Filtering"` and `log_component="Web Content Policy"` and appear in the "Web content policy" module of the Log viewer.

The transactions that appear in this Log have either been blocked or logged due to content that matches a content filter in the corresponding rule. If the content has been scanned but doesn't match any content filter, it does not appear in this log and only appears in the Web Filter Logs.

Central Reporting Format

Log format name under crformatter.conf is `CR_wcp_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Content Filtering	
log_component	N/A	log_component	String			Web Content Policy	
log_subtype	N/A	log_subtype	String		The action taken for the logged transaction	Alert	
severity	N/A	N/A	String				
user_name	Username	user	String	384	The end-user associated with the item being scanned		
src_ip	N/A	src_ip			The IP address of the user trying to download/upload content		
transaction_id	Transaction ID	transaction_id	String	64	Indicates the transaction_id of the AV scan. The same transaction_id appears in the Web Filter logs allowing the admin to view the Web policy decision associated with a particular transaction		eg. transaction_id="e4a127f7-a850-477c-920e-a471b38727c1"
content_filter_key	Content Filter	content_filter_key	String	128	The name of the custom/ predefined content filter matched during content scanning		eg. EthnicitytermsCA
http_category	Site Category	site_category	String	64	The web category of the website accessed		
domain	Website	website	String	512	The domainname of location where content is being downloaded from or uploaded to		
con_direction	Direction	direction	String	64	The direction of the content being scanned	in out	• "in" when content is being downloaded • "out" when content is being uploaded
action	Action	action	String	64	The web policy action taken on the content ,based on the web policy rule	Deny Log	• "Deny" when website is blocked due to content match • "Log" when content matches are logged and acl system continues with policy rules to make he final decision
file_name	Filename	file_name	String	1024	name of the file being downloaded or uploaded		
context_match	Context	context_match	String	128	The string(context) of the file that matches the exact word /words defined in the content Filter		eg. context_match="far"
context_prefix	Context	context_prefix	String	64	The string (context) of the file that precedes the matched content		eg. context_prefix="This place is "
context_suffix	Context	context_suffix	String	64	The string (context) of the file that succeeds the matched content		eg. context_suffix=" from home! "
log_id		N/A	String				eg. "010101600001"
device_name		N/A	String				eg "SFW"
device_model		N/A	String				eg "SF01V"
device_serial_id		N/A	String				eg "SFDemo-ff94e90"
log_version		N/A	Number			1	eg. log_version=1

user_group		N/A					
dst_country	destination country	N/A	string	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"
dst_zone	destination zone	N/A			destination zone		e.g. "WAN"
dst_zone_type	destination zone type	N/A	string		destination zone type (for custom zones)		e.g. "WAN"
src_country	source country	N/A	string	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"
src_zone	source zone	N/A			source zone		e.g. "LAN"
src_zone_type	source zone type	N/A			source zone type (for custom zones)		e.g. "LAN"
dst_ip	Destination IP	N/A			The IP address to which the HTTP/HTTPS connection was made		
src_port	N/A	N/A			The port from which the HTTP/HTTPS connection originated		
dst_port	N/A	N/A			The port to which the HTTP/HTTPS connection was made		

Device Standard Format (legacy)

Log format name under crformatter.conf is `wcp_log_fmt`.

Field descriptions

Syslog field name	Name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Content Filtering	
log_component	N/A	log_component	String			Web Content Policy	
log_subtype	N/A	log_subtype	String		The action taken for the logged transaction	Alert	
priority	N/A	N/A	String				
user_name	Username	user	String	384	The end-user associated with the item being scanned		
src_ip	N/A	src_ip			The IP address of the user trying to download/upload content		
transactionid	Transaction ID	transaction_id	String	64	Indicates the transaction_id of the AV scan. The same transaction_id appears in the Web Filter logs allowing the admin to view the Web policy decision associated with a particular transaction		eg. transaction_id="e4a127f7-a850-477c-920e-a471b38727c1"
dictionaryname	Content Filter	content_filter_key	String	128	The name of the custom/ predefined content filter matched during content scanning		eg. EthnicitytermsCA
sitecategory	Site Category	site_category	String	64	The web category of the website accessed		
website	Website	website	String	512	The domainname of location where content is being downloaded from or uploaded to		
direction	Direction	direction	String	64	The direction of the content being scanned	in out	• "in" when content is being downloaded • "out" when content is being uploaded
action	Action	action	String	64	The web policy action taken on the content ,based on the web policy rule	Deny Log	• "Deny" when website is blocked due to content match • "Log" when content matches are logged and acl system continues with policy rules to make he final decision
filename	Filename	file_name	String	1024	name of the file being downloaded or uploaded		
contextmatch	Context	context_match	String	128	The string(context) of the file that matches the exact word /words defined in the content Filter		eg. context_match="far"

contextprefix	Context	context_prefix	String	64	The string (context) of the file that precedes the matched content		eg. context_prefix="This place is "
contextsuffix	Context	context_suffix	String	64	The string (context) of the file that succeeds the matched content		eg. context_suffix=" from home! "
log_id		N/A	String				eg. "010101600001"
device		N/A	String				eg "SFW"
device_name		N/A	String				eg "SF01V"
device_id		N/A	String				eg "SFDemo-ff94e90"

Sample logs

Message ID	Log
16010	`device_name="SF01V" device_id=SFDemo-c45b327 log_id=058420116010 log_type="Content Filtering" log_component="Web Content Policy" log_subtype="Alert" user="gi123456" src_ip=10.108.108.49 transaction_id="e4a127f7-a850-477c-920e-a471b38727c1" dictionary_name="complicated_Custom" site_category=Information Technology website="ta-web-static-testing.qa.astaro.de" direction="in" action="Deny" file_name="cgi_echo.pl" context_match="Not" context_prefix="blah blah hello " context_suffix=" hello blah "`

Reporting

- Reports under:
  - Web Content: Reports > Applications & Web > Web Content
- Log identifier for reports:
  - Web Content: Log Type = Content Filtering & Log Component = Web Content Policy

Web filter

Web transactions are generally logged with `log_type="Content Filtering"` and appear in the "Web filter" log viewer.

The exception to this is when a transaction is blocked because it contains malware. These transactions are logged using `log_type="Anti-Virus` and `log_subtype="Virus"`.

Central Reporting Format

Field descriptions

Log format name under crformatter.conf is `CR_contflt_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Max length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Content Filtering	
log_component	N/A	log_component	String			HTTP	
log_subtype	Action	log_subtype	String		The action taken for the logged HTTP /HTTPS transaction	Allowed Denied Override Warned Quota	
log_id	N/A	N/A	String		see "Common fields' values and format"		
severity	Severity	N/A	String		Severity of the event	Information	
fw_rule_id	Firewall rule ID	fw_rule_id	Number	int32	Indicates the ID number of the Firewall policy rule that applies to this transaction		
user_name	User name	user	String	384	The end-user associated with the item being scanned		
user_group	User group	user_group	String	1024	The group to which the user belongs		
web_policy_id	Web policy ID	web_policy_id	Number	int16	The numerical ID of the Web Policy applied to this transaction		
http_category	Web category	category	String	64	The category of the URL being requested		e.g. "Information Technology"
http_category_type	Web category type	category_type	String	64	The classification associated with the category		e.g. "Acceptable", "Unproductive", "Objectionable"
url	URL	url	String	1024	The URL being requested		e.g. "https://www.example.com/index.html"
content_type	Content type	content_type	String	64	The MIME-type of the downloaded content		e.g. "text/plain"
override_token	Override token	override_token	String	64	The token generated for an override session:<user ID>-<connecting IP address>_<override session ID>		This field existed before 17.5 but will only get populated starting with 17.5
override_name	Override name	override_name	String	100	Name of the override session		
override_authorizer	Override authorizer	override_authorizer	String	256	Authorizer (creator) of the override session		
src_ip	Source IP	src_ip			The IP address from which the HTTP /HTTPS connection originated		

dst_ip	Destination IP	dst_ip			The IP address to which the HTTP /HTTPS connection was made		
protocol	N/A	protocol	String		IP protocol used fro the connection	"TCP"	
src_port	N/A	src_port			The port from which the HTTP/HTTPS connection originated		
dst_port	N/A	dst_port			The port to which the HTTP/HTTPS connection was made		
bytes_sent	Bytes sent	bytes_sent	Number	int32	Bytes sent upstream to the web server by the firewall		
bytes_received	N/A	bytes_received	Number	int32	Bytes received from the upstream web server by the firewall		This will not necessarily be identical to the bytes sent to the client by the firewall, especially if the content was retrieved from the local web cache.
domain	N/A	domain	String	512	The FQDN part of the URL, representing the hostname/domain of the web site		e.g. "www.google.com"
activity_name	N/A	activity_name	String	64	The name of a Web policy Activity that matched and caused the policy result		If the transaction matches multiple activities then only the first one that causes the policy decision will be recorded
reason	N/A	reason	String	256	For transactions that require Sandstorm analysis, records the Sandstorm status	`eligible`: The file was identified as eligible for Sandstorm analysis but was excluded from analysis. This may be because Sandstorm was disabled in the Firewall rule, in a filetype exclusion, in a Web exception, or because Sandstorm is not licensed `not eligible`: The file was not eligible for Sandstorm analysis because it is not a risky type, or not a type which can be analysed by the Sandstorm cloud service `pending`: The item required analysis in the cloud; the end-user was not able to download the item immediately `cached clean`: The item was previously known to be clean and was allowed `cloud clean`: The item was found to be clean after analysis in the cloud Note that for all items sent to the Sandstorm cloud for analysis, there will be two entries in the "Content Filter" logone with `reason="pending"` when the file is initially requested by the user, and one with `reason="cloud clean"` when the file is known to be OK to download. If the file is found to be malicious, it will be logged in the antivirus log with `reason="cloud malicious"`	
http_user_agent	N/A	user_agent	String	256	The user-agent string for the client.		e.g. "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv: 60.0) Gecko/20100101 Firefox/60.0"
http_status	N/A	status_code	Number	int16	The numeric HTTP response code		e.g. "200"
transaction_id	Transaction ID	transaction_id	String	64	Indicates the AV scan's transaction_id. This will only appear when malware/ content scanning has been performed in that transaction		Corresponds to the av_transaction_id in the awarrenhttp_access logs
http_referer	Referrer	referer	String	512	The HTTP referer header value		e.g. "https://products.office.com/en-us/home"
download_file_name	N/A	download_file_name	String	256	The name of the file that was downloaded.		e.g. "foo.js"
download_file_type	N/A	download_file_type	String	128	The filetype of the file that was downloaded.		e.g. "text/javascript"
upload_file_name	N/A	upload_file_name	String	256	The name of the file that was uploaded.		e.g. "rem.exe"
upload_file_type	N/A	upload_file_type	String	128	The filetype of the file that was uploaded.		e.g. "application/x-msdos-program"
con_id	N/A	con_id	Number	int32	Connection identifier. Used to tie firewall log entries to web filter log entries.		

app_name	N/A	app_name	String	64	Name of application		e.g. "Youtube Website"
app_is_cloud	N/A	app_is_cloud	Number	int16			
used_quota	N/A	used_quota	Number	int16	Used quota time in minutes.		
device_name	device_name	N/A	String				e.g. "SFW"
device_model	device_model	N/A	String				e.g. "SF01V"
device_serial_id		N/A	String				e.g. "S4000806149EE49"
log_version	log version	N/A	NUMBER	int16			e.g. log_version=1
timestamp	timestamp	N/A	TIMESTAMP		ISO 8601		eg timestamp=2018-12-07T10:03:48+0000
dst_country	destination country	N/A	string	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"
dst_zone	destination zone	N/A			destination zone		e.g. "WAN"
dst_zone_type	destination zone type	N/A	string		destination zone type (for custom zones)		e.g. "WAN"
src_country	source country	N/A	string	64	ISO 3166 (A 3) Code		e.g. "IND" "CAN" "USA" "GBR"
src_zone	source zone	N/A			source zone		e.g. "LAN"
src_zone_type	source zone type	N/A			source zone type (for custom zones)		e.g. "LAN"

Device Standard Format

Field descriptions

Log format name under crformatter.conf is `CR_contflt_log_fmt`.

Syslog field name	Name	Log viewer - Detail view field name	Data type	Max length	Format/Description	Possible values	Notes/Examples
log_type	N/A	log_type	String			Content Filtering	
log_component	N/A	log_component	String			HTTP	
log_subtype	Action	log_subtype	String		The action taken for the logged HTTP /HTTPS transaction	Allowed Denied Override Warned Quota	
log_id		N/A	String		see "Common fields' values and format"		
priority	Priority	N/A	String			Information	
fw_rule_id	Firewall rule ID	fw_rule_id	Number	int32	Indicates the ID number of the Firewall policy rule that applies to this transaction		
user_name	User name	user	String	384	The end-user associated with the item being scanned		
user_gp	User group	user_group	String	1024	The group to which the user belongs		
iap	Web policy ID	web_policy_id	Number	int16	The numerical ID of the Web Policy applied to this transaction		
category	Web category	category	String	64	The category of the URL being requested		e.g. "Information Technology"
category_type	Web category type	category_type	String	64	The classification associated with the category		e.g. "Acceptable", "Unproductive", "Objectionable"
url	URL	url	String	1024	The URL being requested		e.g. "https://www.example.com/index.html"
contenttype	Content type	content_type	String	64	The MIME-type of the downloaded content		e.g. "text/plain"
override_token	Override token	override_token	String	64	The token generated for an override session:<user ID>-<connecting IP address>_<override session ID>		This field existed before 17.5 but will only get populated starting with 17.5

override_name	Override name	override_name	String	100	Name of the override session		
override_authorizer	Override authorizer	override_authorizer	String	256	Authorizer (creator) of the override session		
src_ip	Source IP	src_ip			The IP address from which the HTTP /HTTPS connection originated		
dst_ip	Destination IP	dst_ip			The IP address to which the HTTP /HTTPS connection was made		
protocol	N/A	protocol	String		IP protocol used fro the connection	"TCP"	
src_port	N/A	src_port			The port from which the HTTP/HTTPS connection originated		
dst_port	N/A	dst_port			The port to which the HTTP/HTTPS connection was made		
sent_bytes	Bytes sent	bytes_sent	Number	int32	Bytes sent upstream to the web server by the firewall		
recv_bytes	N/A	bytes_received	Number	int32	Bytes received from the upstream web server by the firewall		This will not necessarily be identical to the bytes sent to the client by the firewall, especially if the content was retrieved from the local web cache.
domain	N/A	domain	String	512	The FQDN part of the URL, representing the hostname/domain of the web site		e.g. "www.google.com"
exceptions	N/A	exception	String	64	Comma separated list of the checks excluded by Web Exceptions	`av`: Do not scan for malware `https`: Do not decrypt HTTPS traffic `sandstorm`: Do not check downloaded content with Sandstorm `policy`: Do not apply policy checks (i.e. Allow/Warn/Block by Category, URL Group, Dynamic Category, etc.)	
activityname	N/A	activity_name	String	64	The name of a Web policy Activity that matched and caused the policy result		If the transaction matches multiple activities then only the first one that causes the policy decision will be recorded
reason	N/A	reason	String	256	For transactions that require Sandstorm analysis, records the Sandstorm status	`eligible`: The file was identified as eligible for Sandstorm analysis but was excluded from analysis. This may be because Sandstorm was disabled in the Firewall rule, in a filetype exclusion, in a Web exception, or because Sandstorm is not licensed `not eligible`: The file was not eligible for Sandstorm analysis because it is not a risky type, or not a type which can be analysed by the Sandstorm cloud service `pending`: The item required analysis in the cloud; the end-user was not able to download the item immediately `cached clean`: The item was previously known to be clean and was allowed `cloud clean`: The item was found to be clean after analysis in the cloud Note that for all items sent to the Sandstorm cloud for analysis, there will be two entries in the "Content Filter" logone with `reason="pending"` when the file is initially requested by the user, and one with `reason="cloud clean"` when the file is known to be OK to download. If the file is found to be malicious, it will be logged in the antivirus log with `reason="cloud malicious"`	
user_agent	N/A	user_agent	String	256	The user-agent string for the client.		e.g. "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0"
status_code	N/A	status_code	Number	int16	The numeric HTTP response code		e.g. "200"
transactionid	Transaction ID	transaction_id	String	64	Indicates the AV scan's transaction_id. This will only appear when malware/ content scanning has been performed in that transaction		Corresponds to the av_transaction_id in the awarrenhttp_access logs
referer	Referrer	referer	String	512	The HTTP referer header value		e.g. "https://products.office.com/en-us/home"
download_file_name	N/A	download_file_name	String	256	The name of the file that was downloaded.		e.g. "foo.js"
download_file_type	N/A	download_file_type	String	128	The filetype of the file that was downloaded.		e.g. "text/javascript"
upload_file_name	N/A	upload_file_name	String	256	The name of the file that was uploaded.		e.g. "rem.exe"
upload_file_type	N/A	upload_file_type	String	128	The filetype of the file that was uploaded.		e.g. "application/x-msdos-program"

con_id	N/A	con_id	Number	int32	Connection identifier. Used to tie firewall log entries to web filter log entries.		
application	N/A	app_name	String	64	Name of application		e.g. "Youtube Website"
app_is_cloud	N/A	app_is_cloud	Number	int16			
used_quota	N/A	used_quota	Number	int16	Used quota time in minutes.		
device	N/A		String				e.g. "SFW"
device_name	N/A		String				e.g. "SF01V"
device_id	N/A		String				e.g. "S4000806149EE49"

Sample logs

Message ID	Logs
16001	device="SFW" date=2016-12-02 time=18:27:03 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050901616001 log_type="Content Filtering" log_component="HTTP" log_subtype="Allowed" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="None" category_type="" url="http://floater.baldrys.ca/adsenum.exe" contenttype="application/octet-stream" override_token="" src_ip=192.168.73.220 dst_ip=50.112.191.33 protocol="TCP" src_port=54110 dst_port=80 sent_bytes=0 recv_bytes=15940 domain=floater.baldrys.ca exceptions= activityname="" reason="cached clean" device="SFW" date=2016-12-02 time=18:35:51 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050901616001 log_type="Content Filtering" log_component="HTTP" log_subtype="Allowed" priority=Information fw_rule_id=0 user_name="rich" user_gp="" iap=13 category="None" category_type="" url="http://floater.baldrys.ca/usemem.exe" contenttype="application/octet-stream" override_token="" src_ip=192.168.73.220 dst_ip=192.168.73.220 protocol="TCP" src_port=54110 dst_port=80 sent_bytes=0 recv_bytes=321677 domain=floater.baldrys.ca exceptions= activityname="" reason="cloud clean" device="SFW" date=2016-12-02 time=19:21:41 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050901616001 log_type="Content Filtering" log_component="HTTP" log_subtype="Allowed" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="Information Technology" category_type="Acceptable" url="https://the.earth.li/~sgtatham/putty/0.67/x86/putty.exe" contenttype="application/x-msdos-program" override_token="" httpresponsecode="" src_ip=192.168.73.220 dst_ip=46.43.34.31 protocol="TCP" src_port=51570 dst_port=443 sent_bytes=0 recv_bytes=531659 domain=the.earth.li exceptions= activityname="" reason="eligible" device="SFW" date=2016-12-02 time=19:21:59 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050901616001 log_type="Content Filtering" log_component="HTTP" log_subtype="Allowed" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="General Business" category_type="Acceptable" url="http://ads.adaptv.advertising.com/a/h/WWEVd91PNug3Es_Gwp40Tnr0FIh9nkWQ?cb=1481065476497&pet=preroll&pageUrl=http%3A%2F%2Fbbc.com%2F&eov=eov&a.cluster=0&a.pvt=0&width=300&height=250&a.sdk=adaptv&a.sdkType=js&a.d.pageUrl=http%3A%2F%2Fwww.bbc.com%2Fsport&referrerUrl=http%3A%2F%2Fwww.bbc.com%2Fearth%2Fworld&depth=0&p.vw.active=-1&p.vw.area=-1&p.vw.domId=-1&p.vw.framerate=-1&p.vw.geometric=-1&p.vw.pHeight=0&p.vw.psize=-1&p.vw.pWidth=0&p.vw.viewable=-1&p.vw.viewableOpportunity=-1" contenttype="text/xml" override_token="" src_ip=192.168.73.220 dst_ip=52.9.247.25 protocol="TCP" src_port=56477 dst_port=80 sent_bytes=0 recv_bytes=3672 domain=ads.adaptv.advertising.com exceptions= activityname="" reason="not eligible"
16002	device="SFW" date=2016-12-02 time=18:26:43 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050902616002 log_type="Content Filtering" log_component="HTTP" log_subtype="Denied" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="None" category_type="" url="http://floater.baldrys.ca/badb.exe" contenttype="application/octet-stream" override_token="" src_ip=192.168.73.220 dst_ip=50.112.191.33 protocol="TCP" src_port=54110 dst_port=80 sent_bytes=0 recv_bytes=1594715 domain=floater.baldrys.ca exceptions= activityname="" reason="pending" device="SFW" date=2016-12-02 time=19:30:33 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050902616002 log_type="Content Filtering" log_component="HTTP" log_subtype="Denied" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=14 category="Financial Services" category_type="Unproductive" url="https://www.vancity.com/" contenttype="" override_token="" src_ip=192.168.73.220 dst_ip=208.69.252.169 protocol="TCP" src_port=60444 dst_port=443 sent_bytes=0 recv_bytes=0 domain=www.vancity.com exceptions= activityname="Finance & Investing" reason=""

16003	
16005	device="SFW" date=2016-12-02 time=18:50:20 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050927616005 log_type="Content Filtering" log_component="HTTP" log_subtype="Warned" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="Search Engines" category_type="Acceptable" url="http://www.google.com/" contenttype="" override_token="" src_ip=192.168.73.220 dst_ip=64.233.189.147 protocol="TCP" src_port=37832 dst_port=80 sent_bytes=0 recv_bytes=0 domain=www.google.com exceptions= activityname="Search" reason=""
16006	device="SFW" date=2016-12-02 time=18:50:22 timezone="GMT" device_name="SFVUNL" device_id=C01001K234RXPA1 log_id=050901616006 log_type="Content Filtering" log_component="HTTP" log_subtype="Allowed" priority=Information fw_rule_id=2 user_name="rich" user_gp="Clientless Open Group" iap=13 category="Search Engines" category_type="Acceptable" url="http://www.google.ca/?gfe_rd=cr&ei=ojxHWP3WC4WN8QeRioDABw" contenttype="text/html" override_token="" src_ip=192.168.73.220 dst_ip=64.233.188.94 protocol="TCP" src_port=46322 dst_port=80 sent_bytes=0 recv_bytes=619 domain=www.google.ca exceptions= activityname="Search" reason="not eligible"

Reporting

- Reports under:
  - Web Allowed: Reports > Application & Web > Web Risks & Usage
  - Web Denied: Reports > Application & Web > Blocked Web Attempts
  - Also use to report:
    - CASB (With combination of Application Logs): Reports > Application & Web > Cloud Application Usage
    - Search Engine (Where URL has search pattern): Reports > Application & Web > Search Engine
- Log identifier for reports:
  - Web Allowed: Log Component = HTTP & (Log Subtype = Allowed or Clean or Warned)
  - Web Denied: Log Component = HTTP & Log Subtype = Denied

Wireless

Log format name under crformatter.conf is `wc_log_fmt`.

Field descriptions

Syslog field name	Log viewer - Detail view field name	Data type	Length	Format/Description	Possible values	Notes /Examples
log_type	log_type	String		It is a log type.	Wireless Protection	
log_component	log_component	String		It is a log component.	Wireless Protection	
log_subtype	log_subtype	String		It is a sub type.	Information	
priority		String		It is a priority of the message content.	Information	
ap	AP_SN	String	64	It is Access Point serial ID or LocalWifi0 or LocalWifi1	Access Point Serial ID or LocalWifi0 or LocalWifi1	
ssid	SSID	String	64	It is SSID name.	configured SSID name	
clients_conn_SSID	connected_client_count	Number	int32	Number of client connected for that SSID.	clients_conn_SSID= (No. of connected client count)	

Reporting

- Reports under:
  - Wireless: Reports > Network & Threats > Wireless
- Log identifier for reports:
  - Wireless: Log Type = Wireless Protection & Log Component = Wireless Protection

Sample logs

Message ID	Log

18011	`device="SFW" date=2017-02-01 time=14:17:35 timezone="IST" device_name="SG115" device_id=S110016E28BA631 log_id=106025618011 log_type="Wireless Protection" log_component=" Wireless Protection" log_subtype="Information" priority=Information ap=A40024A636F7862 ssid=SPIDIGO2015 clients_conn_SSID=2`
	
	`device="SFW" date=2017-02-01 time=14:19:47 timezone="IST" device_name="SG115" device_id=S110016E28BA631 log_id=106025618011 log_type="Wireless Protection" log_component=" Wireless Protection" log_subtype="Information" priority=Information ap=A40024A636F7862 ssid=SPIDIGO2015 clients_conn_SSID=3`