

SOPHOS

Cybersecurity
made
simple.

SF syslog file guide 19.0 - Firewall

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		
fw_rule_name	fw_rule_name	String		Firewall rule name 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, "Trill"}, {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"}, {0x8888, "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, "TTTEthernet 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)"}, {0xCAFÉ, "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		
nat_rule_id	nat_rule_id	Number	int32	NAT rule ID used for particular request		
nat_rule_name	nat_rule_name	String		NAT rule name used for particular request		

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

Messa ge 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 rcv_pkts=0 sent_bytes=0 rcv_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 rcv_pkts=0 sent_bytes=0 rcv_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="" 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 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: <pre>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"</pre>
2001	Not found in code.
2002	<pre>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"</pre>
3001	<pre>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"</pre>
4001	<pre>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"</pre>
5001	<pre>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"</pre>
5051	<pre>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"</pre>

5101	device="SFW" date=2018-05-30 time=15:12:45 timezone="IST" device_name="XG125w" device_id=SF Demo-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 rcv_pkts=0 sent_bytes=0 rcv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczone="" srczone="" dstzone="" 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=SF Demo-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 rcv_pkts=0 sent_bytes=0 rcv_bytes=0 tran_src_ip= tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczone="" srczone="" dstzone="" 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=2023-12-14 time=05:19:43 timezone="EST" device_name="SF01V" device_id=SF Demo-c07-gulzar-multilink-01 log_id=010101600001 log_type="Firewall" log_component="Firewall Rule" log_subtype="Allowed" status="Allow" priority=Information duration=0 fw_rule_id=5 fw_rule_name="fw_allow_11.11.11.3" fw_rule_section="Local rule" nat_rule_id=3 nat_rule_name="nat_allow_11.11.11.3" policy_type=1 sdwan_profile_id_request=0 sdwan_profile_name_request="" 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=0 sdwan_route_name_request="" 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="Port2" in_display_interface="Port2" out_interface="Port1" out_display_interface="Port1" src_mac=00:50:56:B0:29:5E dst_mac=00:50:56:B0:1A:7B src_ip=11.11.11.3 src_country_code=USA dst_ip=4.2.2.2 dst_country_code=USA protocol="ICMP" icmp_type=8 icmp_code=0 sent_pkts=0 rcv_pkts=0 sent_bytes=0 rcv_bytes=0 tran_src_ip=10.170.0.151 tran_src_port=0 tran_dst_ip= tran_dst_port=0 srczone="LAN" srczone="LAN" dstzone="WAN" dstzone="WAN" dir_disp="" connevent="Start" connid="1159788104" vconnid="" hb_health="No Heartbeat" message="" appresolvedby="Signature" app_is_cloud=0 log_occurrence=1 flags=0