

1. IPS Event in Syslog

Request Details	
Summary	Input
Event:Destination-IP-Address	172.65.203.203
Event:Event-Name	"FGT- syslog"
Event:Fortinet-Events:action	"dropped"
Event:Fortinet-Events:attack	"Adobe.Reader.Printf.Buffer.Overflow"
Event:Fortinet-Events:attack_id	16044
Event:Fortinet-Events:cr_action	4096
Event:Fortinet-Events:cr_level	"critical"
Event:Fortinet-Events:cr_score	50
Event:Fortinet-Events:destination_interface	"port1"
Event:Fortinet-Events:destination_interface_role	"undefined"
Event:Fortinet-Events:destination_ip	172.65.203.203
Event:Fortinet-Events:destination_port	80
Event:Fortinet-Events:devname	"FGT- syslog"
Event:Fortinet-Events:direction	"incoming"
Event:Fortinet-Events:eventtype	"signature"
Event:Fortinet-Events:host	cppm-84.arubasecurity.hpe.com
Event:Fortinet-Events:hostname	"fedeploycheck.fireeye.com"
Event:Fortinet-Events:incident_serial_number	84945375
Event:Fortinet-Events:level	"alert"
Event:Fortinet-Events:msg	"applications2: Adobe.Reader.Printf.Buffer.Overflow,"
Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:profile	"default"
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:ref	"http://www.fortinet.com/ids/VID16044"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	123061
Event:Fortinet-Events:severity	"critical"
Event:Fortinet-Events:source_country	"Reserved"
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	58780
Event:Fortinet-Events:subtype	"ips"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:url	"/appliance-test/test-infection.pdf"
Event:Fortinet-Events:vd	"root"
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17

◀ Showing 4 of 1-6 records ▶

Change Status

Show Configuration

Export

Show Logs

Close

2. Application Control in Syslog

Request Details	
Summary	Input
Event:Destination-IP-Address	45.33.83.49
Event:Event-Name	"FGT- syslog"
Event:Fortinet-Events:action	"accept"
Event:Fortinet-Events:app	"BitTorrent"
Event:Fortinet-Events:app_act	"drop-session"
Event:Fortinet-Events:app_category	"P2P"
Event:Fortinet-Events:appid	6
Event:Fortinet-Events:app_list	"block-high-risk"
Event:Fortinet-Events:app_risk	"high"
Event:Fortinet-Events:destination_country	"United States"
Event:Fortinet-Events:destination_interface	"port1"
Event:Fortinet-Events:destination_interface_role	"undefined"
Event:Fortinet-Events:destination_ip	45.33.83.49
Event:Fortinet-Events:destination_port	6969
Event:Fortinet-Events:devname	"FGT- syslog"
Event:Fortinet-Events:host	c ppm-84.arubasecurity.hpe.com
Event:Fortinet-Events:level	"notice"
Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:policy_name	"Allow Kali outbound"
Event:Fortinet-Events:policy_type	"policy"
Event:Fortinet-Events:policy_uuid	"6f076092-5c5f-51ed-6271- 4dcc437f9479"
Event:Fortinet-Events:proto	17
Event:Fortinet-Events:service	"udp/6969"
Event:Fortinet-Events:session_id	121799
Event:Fortinet-Events:source_country	"Reserved"
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	51413
Event:Fortinet-Events:subtype	"forward"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:trandisp	"noop"
Event:Fortinet-Events:vd	"root"
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17
Event:Timestamp	2022-11-09 13:01:22
Event:Username	hulk

Showing 3 of 1-6 records

Change Status

Show Configuration

Export

Show Logs

Close

3. AntiVirus in Syslog

Request Details	
Summary	Input
Event:Destination-IP-Address	208.94.116.21
Event:Event-Name	"FGT- syslog"
Event:Fortinet-Events:action	"monitored"
Event:Fortinet-Events:destination_interface	"port1"
Event:Fortinet-Events:destination_interface_role	"undefined"
Event:Fortinet-Events:destination_ip	208.94.116.21
Event:Fortinet-Events:destination_port	80
Event:Fortinet-Events:devname	"FGT- syslog"
Event:Fortinet-Events:direction	"incoming"
Event:Fortinet-Events:dtype	"Virus"
Event:Fortinet-Events:eventtype	"infected"
Event:Fortinet-Events:filename	"ms14_064_ole_xp.html"
Event:Fortinet-Events:host	cppm-84.arubasecurity.hpe.com
Event:Fortinet-Events:level	"notice"
Event:Fortinet-Events:msg	"File is infected."
Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:quarantine_skip	"Quarantine-disabled"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	136652

ClearPass-Fortinet Ingress Events

Event:Fortinet-Events:quarantine_skip	"Quarantine-disabled"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	136652
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	42830
Event:Fortinet-Events:subtype	"virus"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:vd	"root"
Event:Fortinet-Events:virus	"VBS/Agent.QSF!tr.dldr"
Event:Fortinet-Events:virus_id	8160367
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17
Event:Timestamp	2022-11-09 13:02:30
Event:Username	hulk
Tips:Service	Ingress-Event

◀ Showing 2 of 1-6 records ▶▶

Change Status

Show Configuration

Export

Show Logs

Close

4. Malicious Website Test

Request Details

Summary	Input	Output
Event:Destination-IP-Address	50.63.7.226	
Event:Event-Name	"FGT- syslog"	
Event:Fortinet-Events:action	"blocked"	
Event:Fortinet-Events:category_description	"Malicious Websites"	
Event:Fortinet-Events:cr_action	4194304	
Event:Fortinet-Events:cr_level	"high"	
Event:Fortinet-Events:cr_score	30	
Event:Fortinet-Events:destination_interface	"port1"	
Event:Fortinet-Events:destination_interface_role	"undefined"	
Event:Fortinet-Events:destination_ip	50.63.7.226	
Event:Fortinet-Events:destination_port	80	
Event:Fortinet-Events:devname	"FGT- syslog"	
Event:Fortinet-Events:eventtype	"ftgd_blk"	
Event:Fortinet-Events:host	cppm-84.arubasecurity.hpe.com	
Event:Fortinet-Events:hostname	"maliciouswebsitetest.com"	
Event:Fortinet-Events:level	"warning"	
Event:Fortinet-Events:policy_id	1	
Event:Fortinet-Events:profile	"Custom"	
Event:Fortinet-Events:proto	6	
Event:Fortinet-Events:req_type	"direct"	

ClearPass-Fortinet Ingress Events

Event:Fortinet-Events:policy_id	1
Event:Fortinet-Events:profile	"Custom"
Event:Fortinet-Events:proto	6
Event:Fortinet-Events:req_type	"direct"
Event:Fortinet-Events:service	"HTTP"
Event:Fortinet-Events:session_id	133792
Event:Fortinet-Events:source_interface	"port2"
Event:Fortinet-Events:source_interface_role	"undefined"
Event:Fortinet-Events:source_ip	172.16.99.17
Event:Fortinet-Events:source_port	53314
Event:Fortinet-Events:subtype	"webfilter"
Event:Fortinet-Events:syslog_priority	13
Event:Fortinet-Events:url	"http://maliciouswebsitetest.com/"
Event:Fortinet-Events:vd	"root"
Event:MAC-Address	7e054b7e8c35
Event:Pattern-Name	Fortinet-Events
Event:Source-IP-Address	172.16.99.17
Event:Timestamp	2022-11-09 13:03:20
Event:Username	hulk

◀ Showing 1 of 1-6 records ▶▶

Change Status

Show Configuration

Export

Show Logs

Close