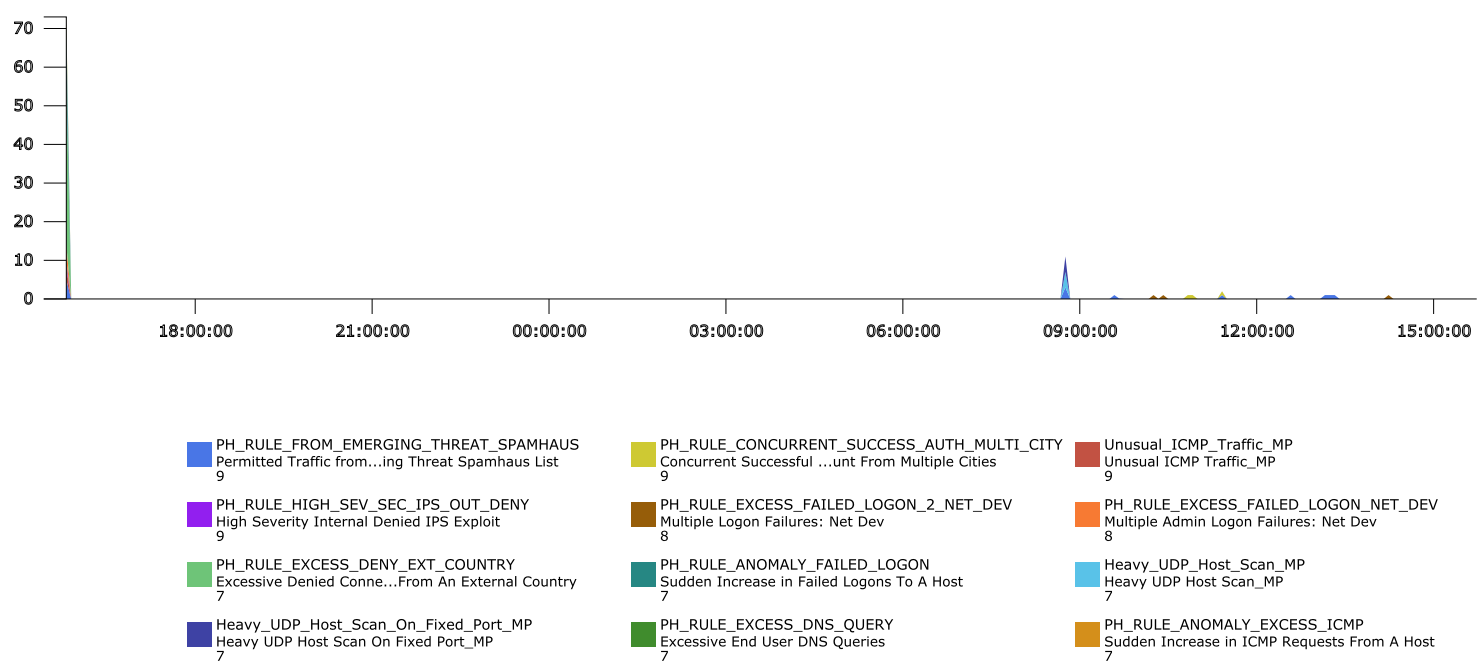
MP LogReview: Top Security Incidents By Severity, Count

Organization: Super/Global

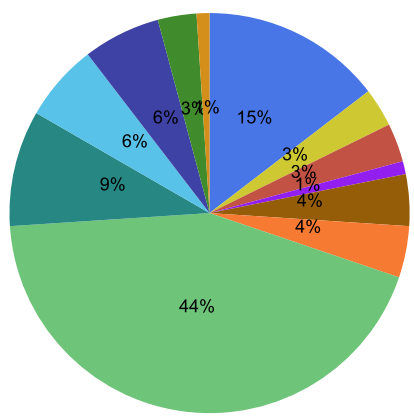
Time Range 4/5/15 3:48:52 PM to 4/6/15 3:48:51 PM
Generated 4/6/15 3:49:07 PM
Description Ranks the security related incidents by first their severity and then by their count

User Notes

Trend Chart for COUNT(Matched Events)



Pie Chart for COUNT(Matched Events)



Found 14

Rank	Event Type	Event Name	Event Severity	COUNT(Matched Events)
1	PH_RULE_FROM_EMERGING_THREAT_SPAMHAUS	Permitted Traffic from Emerging Threat Spamhaus List	9	14
2	PH_RULE_CONCURRENT_SUCCESS_AUTH_MULTI_CITY	Concurrent Successful Authentications To Same Account From Multiple Cities	9	3
3	Unusual_ICMP_Traffic_MP	Unusual ICMP Traffic_MP	9	3
4	PH_RULE_HIGH_SEV_SEC_IPS_OUT_DENY	High Severity Internal Denied IPS Exploit	9	1
5	PH_RULE_EXCESS_FAILED_LOGON_2_NET_DEV	Multiple Logon Failures: Net Dev	8	4
6	PH_RULE_EXCESS_FAILED_LOGON_NET_DEV	Multiple Admin Logon Failures: Net Dev	8	4
7	PH_RULE_EXCESS_DENY_EXT_COUNTRY	Excessive Denied Connections From An External Country	7	42
8	PH_RULE_ANOMALY_FAILED_LOGON	Sudden Increase in Failed Logons To A Host	7	9
9	Heavy_UDP_Host_Scan_MP	Heavy UDP Host Scan_MP	7	6
10	Heavy_UDP_Host_Scan_On_Fixed_Port_MP	Heavy UDP Host Scan On Fixed Port_MP	7	6
11	PH_RULE_EXCESS_DNS_QUERY	Excessive End User DNS Queries	7	3
12	PH_RULE_ANOMALY_EXCESS_ICMP	Sudden Increase in ICMP Requests From A Host	7	1
13	PH_RULE_ANOMALY_TRAFFIC_DENIED_INBOUND_PORT	Sudden Increase In Denied Inbound Traffic To A Specific TCP/UDP port	7	1
14	PH_RULE_HIGH_SEV_SEC_IPS_IN_DENY	High Severity Inbound Denied IPS Exploit	5	670

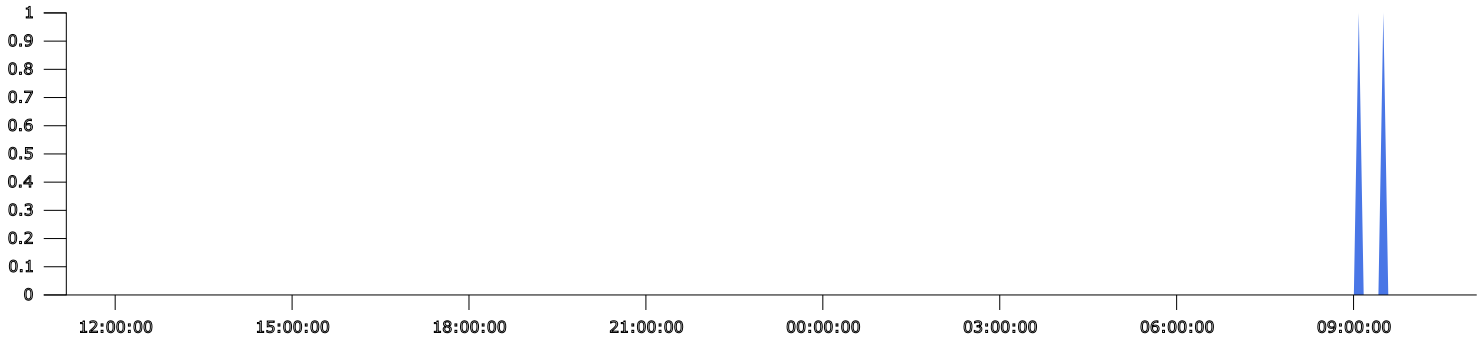
MP LogReview: Rogue Access Point Detection v.2a

Organization: Super/Global

Time Range 1/25/15 11:05:19 AM to 1/26/15 11:05:19 AM
Generated 4/6/15 11:07:40 AM
Description Rogue access points detected through Fortinet sensors on WAPs.

User Notes
Ran this is the data range of the event provided by Dan.

Trend Chart for COUNT(Matched Events)



Bar Chart for COUNT(Matched Events)

Records 2

Rank	Event Receive Time	Reporting IP	Event Type	Event Name	Source IP	Destination IP	User defined msg	WLAN SSID	Raw Event
1	Mon Jan 26 09:04:39 PST 2015	10.151.4.33	FortiGate-wireless-rogue-ap-on-wire	FortiGate-wireless-rogue-ap-on-wire			AP ROGUE-ONWIRE e0:91:f5:ec:50:a4 MAA e0:91:f5:ec:50:a5	ROGUE-ONWIRE	<188>date=2015-01-26 time=09:04:39 devname=FWF60D4614004026 devid=FWF60D4614004026 logid=0104043525 type=event subtype=wireless level=warning vd="root" ssid="ROGUE-ONWIRE" bssid=e0:91:f5:ec:50:a4 aptype=0 rate=72 radioband=802.11n channel=11 action="rogue-ap-on-wire" manuf="NETGEAR" securitymode="WPA Auto" signal=-24 noise=-95 live=43 age=40 onwire=yes detectionmethod="mac adjacency" stamac=e0:91:f5:ec:50:a5 apscan="N/A" sndetected="N/A" radioiddetected=0 stacount=0 snclosest="FWF60D4614004026" radioidclosest=0 apstatus=0 msg="AP ROGUE-ONWIRE e0:91:f5:ec:50:a4 MAA e0:91:f5:ec:50:a5"
2	Mon Jan 26 09:27:11 PST 2015	10.151.4.33	FortiGate-wireless-rogue-ap-on-wire	FortiGate-wireless-rogue-ap-on-wire			AP ROGUE-ONWIRE e0:91:f5:ec:50:a4 MAA e0:91:f5:ec:50:a5	ROGUE-ONWIRE	<188>date=2015-01-26 time=09:27:11 devname=FWF60D4614004026 devid=FWF60D4614004026 logid=0104043525 type=event subtype=wireless level=warning vd="root" ssid="ROGUE-ONWIRE" bssid=e0:91:f5:ec:50:a4 aptype=0 rate=72 radioband=802.11n channel=11 action="rogue-ap-on-wire" manuf="NETGEAR" securitymode="WPA Auto" signal=-23 noise=-95 live=86 age=83 onwire=yes detectionmethod="mac adjacency" stamac=e0:91:f5:ec:50:a5 apscan="N/A" sndetected="N/A" radioiddetected=0 stacount=0 snclosest="FWF60D4614004026" radioidclosest=0 apstatus=0 msg="AP ROGUE-ONWIRE e0:91:f5:ec:50:a4 MAA e0:91:f5:ec:50:a5"

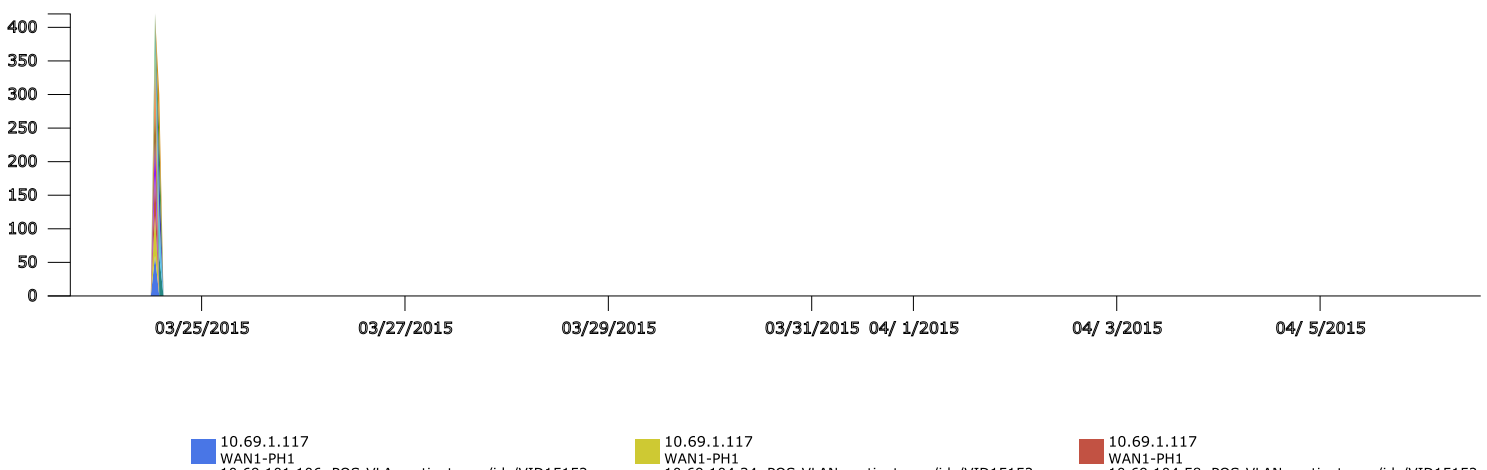
MP LogReview: IPS Events v2.2

Organization: Super/Global

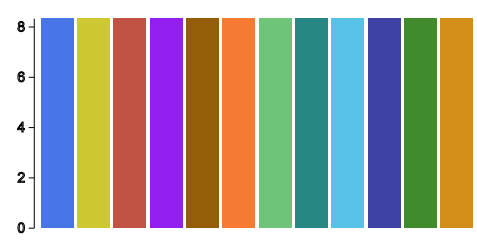
Time Range 3/23/15 2:01:00 PM to 4/6/15 2:00:59 PM
Generated 4/6/15 2:01:19 PM
Description IPS Event where the traffic was not dropped.

User Notes

Trend Chart for Events



Bar Chart for Events



Found 109

Rank	Source IP	Source Intf Name	Destination IP	Destination Intf Name	Service	Event Action	Description	Informational URL	Events
1	10.69.1.117	WAN1-PH1	10.69.101.106	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
2	10.69.1.117	WAN1-PH1	10.69.104.34	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
3	10.69.1.117	WAN1-PH1	10.69.104.58	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
4	10.69.1.117	WAN1-PH1	10.69.105.10	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
5	10.69.1.117	WAN1-PH1	10.69.105.11	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
6	10.69.1.117	WAN1-PH1	10.69.113.106	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
7	10.69.1.117	WAN1-PH1	10.69.115.26	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
8	10.69.1.117	WAN1-PH1	10.69.120.2	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
9	10.69.1.117	WAN1-PH1	10.69.120.58	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
10	10.69.1.117	WAN1-PH1	10.69.120.90	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
11	10.69.1.117	WAN1-PH1	10.69.140.74	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
12	10.69.1.117	WAN1-PH1	10.69.170.10	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
13	10.69.1.117	WAN1-PH1	10.69.181.74	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
14	10.69.1.117	WAN1-PH1	10.69.181.114	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
15	10.69.1.117	WAN1-PH1	10.69.181.122	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
16	10.69.1.117	WAN1-PH1	10.69.182.58	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
17	10.69.1.117	WAN1-PH1	10.69.187.138	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
18	10.69.1.117	WAN1-PH1	10.140.84.75	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
19	10.69.1.117	WAN1-PH1	10.165.84.75	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
20	10.69.1.117	WAN1-PH1	10.165.92.75	POS-VLAN	http	0	web_server: MS.IIS.Web. Server.Folder.Traversal. Evasion.	http://www.fortinet. com/ids/VID15152	60
21	10.69.1.117	WAN1-PH1	10.69.101.106	POS-VLAN	http	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
22	10.69.1.117	WAN1-PH1	10.69.104.34	POS-VLAN	5800/tcp	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
23	10.69.1.117	WAN1-PH1	10.69.104.34	POS-VLAN	http	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
24	10.69.1.117	WAN1-PH1	10.69.104.58	POS-VLAN	http	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
25	10.69.1.117	WAN1-PH1	10.69.105.10	POS-VLAN	5800/tcp	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
26	10.69.1.117	WAN1-PH1	10.69.105.10	POS-VLAN	http	0	web_server: HTTP.URI. Script.XSS.	http://www.fortinet. com/ids/VID10574	29
27	10.69.1.117	WAN1-PH1	10.69.105.11	POS-VLAN	5800/tcp	0	web_server: HTTP.URI.	http://www.fortinet.	29

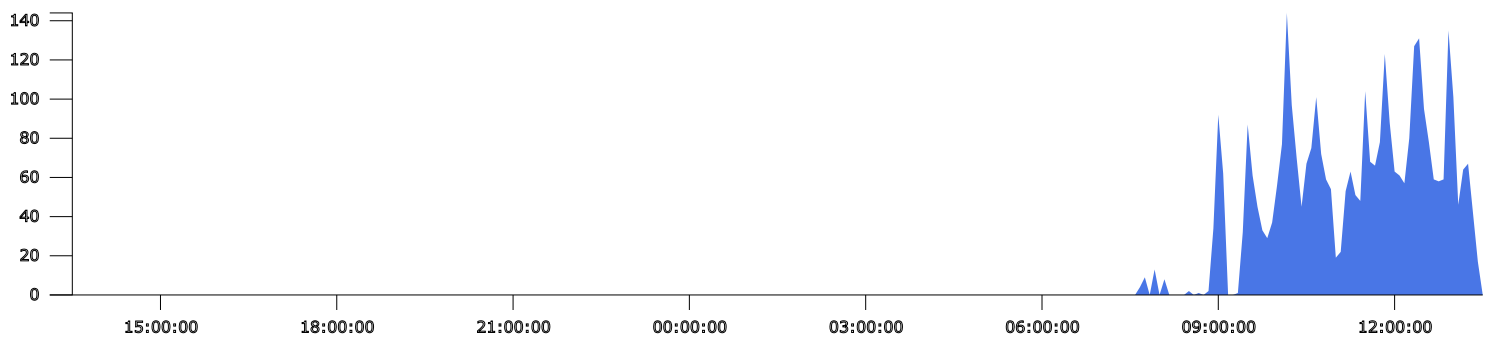
MP LogReview: Detailed Failed Login

Organization: Super/Global

Time Range 4/5/15 1:25:01 PM to 4/6/15 1:25:00 PM
Generated 4/6/15 1:25:25 PM
Description Captures detailed failed logins at any device or application - servers, network devices, domain controllers, VPN gateways, WLAN controllers and applications

User Notes

Trend Chart for COUNT(Matched Events)



Bar Chart for COUNT(Matched Events)

Records 2000

Rank	Event Receive Time	Reporting IP	Event Type	Event Name	Source IP	Source MAC	User	Domain	Raw Event
1	Mon Apr 06 07:39:05 PDT 2015	7.41.79.16	FortiGate-event-login-failure	Failed admin logon	45.56.77.4		hosting		<185>date=2015-04-06 time=07:53:15 devname=PAPA-TX-CLEB-381725 device_id=FW80CM3909633472 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="hosting" ui=ssh(45.56.77.4) action=login status=failed reason=" authentication_failure" msg="Administrator hosting login failed from ssh(45.56.77.4) because of authentication failure"
2	Mon Apr 06 07:39:19 PDT 2015	7.24.14.37	FortiGate-event-login-failure	Failed admin logon	43.255.191.180		root		<185>date=2015-04-06 time=06:30:10 devname=PAPA-MO-COLU-71096 device_id=FW80CM3911601171 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(43.255.191.180) action=login status=failed reason=" authentication_failure" msg="Administrator root login failed from ssh(43.255.191.180) because of authentication failure"
3	Mon Apr 06 07:39:21 PDT 2015	7.24.14.37	FortiGate-event-login-failure	Failed admin logon	43.255.191.180		root		<185>date=2015-04-06 time=06:30:11 devname=PAPA-MO-COLU-71096 device_id=FW80CM3911601171 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(43.255.191.180) action=login status=failed reason=" authentication_failure" msg="Administrator root login failed from ssh(43.255.191.180) because of authentication failure"
4	Mon Apr 06 07:39:22 PDT 2015	7.24.14.37	FortiGate-event-login-failure	Failed admin logon	43.255.191.180		root		<185>date=2015-04-06 time=06:30:12 devname=PAPA-MO-COLU-71096 device_id=FW80CM3911601171 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(43.255.191.180) action=login status=failed reason=" authentication_failure" msg="Administrator root login failed from ssh(43.255.191.180) because of authentication failure"
5	Mon Apr 06 07:40:16 PDT 2015	7.24.12.230	FortiGate-event-login-failure	Failed admin logon	45.56.77.4		hosting		<185>date=2015-04-06 time=07:37:32 devname=PAPA-TX-AUST-68897 device_id=FW80CM3911601532 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="hosting" ui=ssh(45.56.77.4) action=login status=failed reason=" authentication_failure" msg="Administrator hosting login failed from ssh(45.56.77.4) because of authentication failure"
6	Mon Apr 06 07:43:52 PDT 2015	7.34.225.124	FortiGate-event-login-failure	Failed admin logon	195.3.144.115		admin		<185>date=2015-04-06 time=06:46:55 devname=PAPA-TX-DALL-292669 device_id=FW80CM3911604293 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="admin" ui=ssh(195.3.144.115) action=login status=failed reason=" passwd_invalid" msg="Administrator admin login failed from ssh(195.3.144.115) because of invalid password"
7	Mon Apr 06 07:44:14 PDT 2015	7.45.213.54	FortiGate-event-login-failure	Failed admin logon	117.40.239.54		user		<185>date=2015-04-06 time=06:44:17 devname=PAPA-VA-FERR-513689 device_id=FW80CM3914600631 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="user" ui=ssh(117.40.239.54) action=login status=failed reason="ip_blocked" msg="Administrator user login failed from ssh(117.40.239.54) because of blocked IP"
8	Mon Apr 06 07:44:18 PDT 2015	7.45.213.54	FortiGate-event-login-failure	Failed admin logon	117.40.239.54		root		<185>date=2015-04-06 time=06:44:21 devname=PAPA-VA-FERR-513689 device_id=FW80CM3914600631 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(117.40.239.54) action=login status=failed reason="ip_blocked" msg="Administrator root login failed from ssh(117.40.239.54) because of blocked IP"
9	Mon Apr 06 07:44:21 PDT 2015	7.45.213.54	FortiGate-event-login-failure	Failed admin logon					<185>date=2015-04-06 time=06:44:24 devname=PAPA-VA-FERR-513689 device_id=FW80CM3914600631 log_id=0104032002 type=event subtype=admin pri=alert vd=root ui=117.40.239.54 action=login status=failed reason=exceed_limit msg="Login disabled from IP 117.40.239.54 for 60 seconds because of too many bad attempts"
10	Mon Apr 06 07:44:21 PDT 2015	7.45.213.54	FortiGate-event-login-failure	Failed admin logon	117.40.239.54		root		<185>date=2015-04-06 time=06:44:24 devname=PAPA-VA-FERR-513689 device_id=FW80CM3914600631 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(117.40.239.54) action=login status=failed reason="ip_blocked" msg="Administrator root login failed from ssh(117.40.239.54) because of blocked IP"
11	Mon Apr 06 07:44:45 PDT 2015	7.24.15.199	FortiGate-event-login-failure	Failed admin logon	43.255.190.126		root		<185>date=2015-04-06 time=06:43:49 devname=PAPA-TX-AUST-287854 device_id=FW80CM3911604313 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(43.255.190.126) action=login status=failed reason=" passwd_invalid" msg="Administrator root login failed from ssh(43.255.190.126) because of invalid password"
12	Mon Apr 06 07:44:46 PDT 2015	7.24.13.140	FortiGate-event-login-failure	Failed admin logon	117.40.239.54		root		<185>date=2015-04-06 time=07:39:00 devname=PAPA-TX-SANM-278757 device_id=FW80CM3911603655 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(117.40.239.54) action=login status=failed reason=" authentication_failure" msg="Administrator root login failed from ssh(117.40.239.54) because of authentication failure"
13	Mon Apr 06 07:44:47 PDT 2015	7.24.15.199	FortiGate-event-login-failure	Failed admin logon	43.255.190.126		root		<185>date=2015-04-06 time=06:43:51 devname=PAPA-TX-AUST-287854 device_id=FW80CM3911604313 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(43.255.190.126) action=login status=failed reason=" passwd_invalid" msg="Administrator root login failed from ssh(43.255.190.126) because of invalid password"
14	Mon Apr 06 07:53:23 PDT 2015	7.41.77.60	FortiGate-event-login-failure	Failed admin logon	58.218.204.245		root		<185>date=2015-04-06 time=06:53:31 devname=PAPA-IN-GREE-200598 device_id=FW80CM3911603682 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(58.218.204.245) action=login status=failed reason=" passwd_invalid" msg="Administrator root login failed from ssh(58.218.204.245) because of invalid password"
15	Mon Apr 06 07:53:23 PDT 2015	7.24.15.95	FortiGate-event-login-failure	Failed admin logon	221.229.166.28		root		<185>date=2015-04-06 time=07:46:52 devname=PAPA-NJ-HILL-237540 device_id=FW80CM3911603301 log_id=0104032002 type=event subtype=admin pri=alert vd=root user="root" ui=ssh(221.229.166.28) action=login status=failed reason=" authentication_failure" msg="Administrator root login failed from ssh(221.229.166.28) because of authentication failure"
16	Mon Apr 06 07:53:25	7.24.15.79	FortiGate-event-	Failed admin logon	221.229.166.28		root		<185>date=2015-04-06 time=07:54:44 devname=PAPA-MD-CAPI-286250