

FortiGate

FortiGate Daily Security Report

Report Date: 2016-12-31

Data Range: Dec 30, 2016 (FG-61E)

Vdom: root

FORTINET.

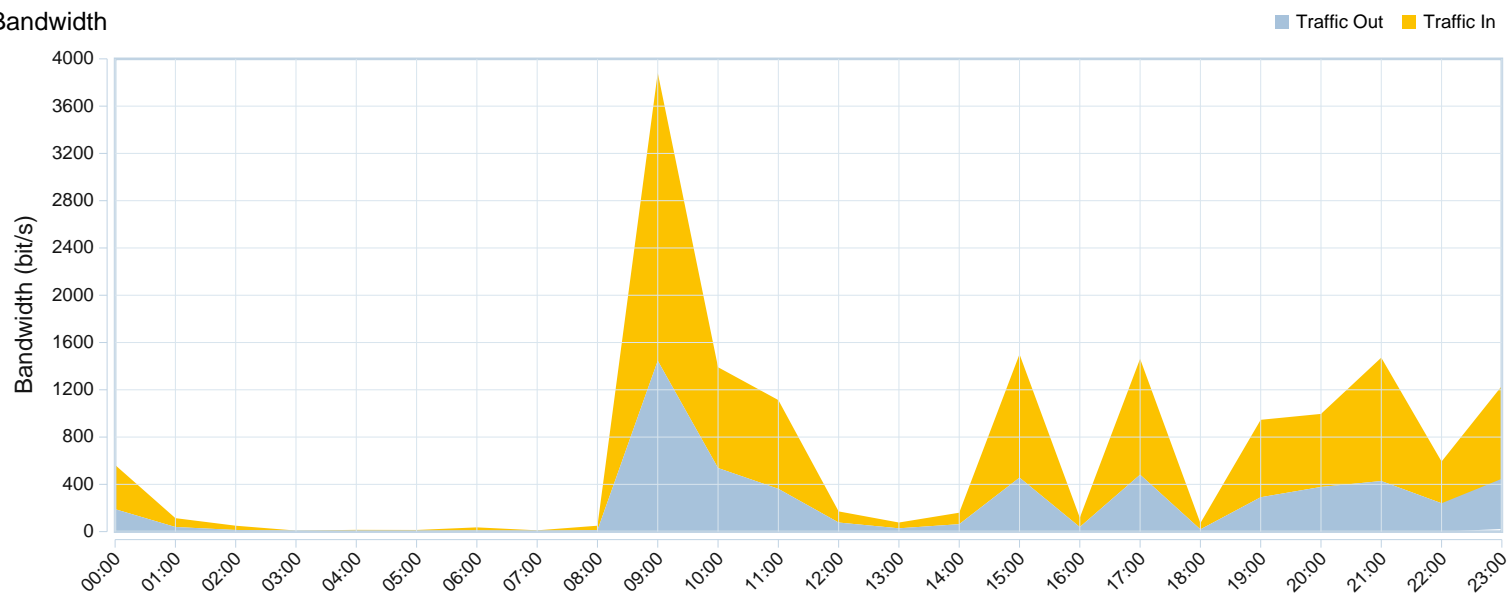
Table of Contents

Bandwidth and Applications.....	1
Bandwidth.....	1
Number of Sessions.....	1
Traffic Statistics.....	2
Top Applications by Bandwidth.....	2
Top Application Categories by Bandwidth.....	2
Top Users by Bandwidth.....	2
Number of Active Users.....	3
Top Destinations by Bandwidth.....	3
Web Usage.....	4
Top Allowed Websites.....	4
Top Websites by Bandwidth.....	4
Top Blocked Websites.....	4
Top Users by Blocked Requests.....	4
Top Users by Requests.....	4
Top Users by Bandwidth.....	4
Top Video Streaming Web Sites by Bandwidth.....	4
Emails.....	5
Top Senders by Number of Emails.....	5
Top Senders by Combined Email Size.....	5
Top Recipients by Number of Emails.....	5
Top Recipients by Combined Email Size.....	5
Threats.....	6
Malware Detected.....	6
Malware Victims.....	6
Malware Sources.....	6
Malware History.....	6
Botnet Detected.....	6
Botnet Victims.....	6
Botnet C&C.....	7
Botnet History.....	7
Intrusions Detected.....	7
Intrusion Victims.....	7
Intrusion Sources.....	7
Intrusions Blocked.....	7
Intrusions By Severity.....	8
Intrusion History.....	8

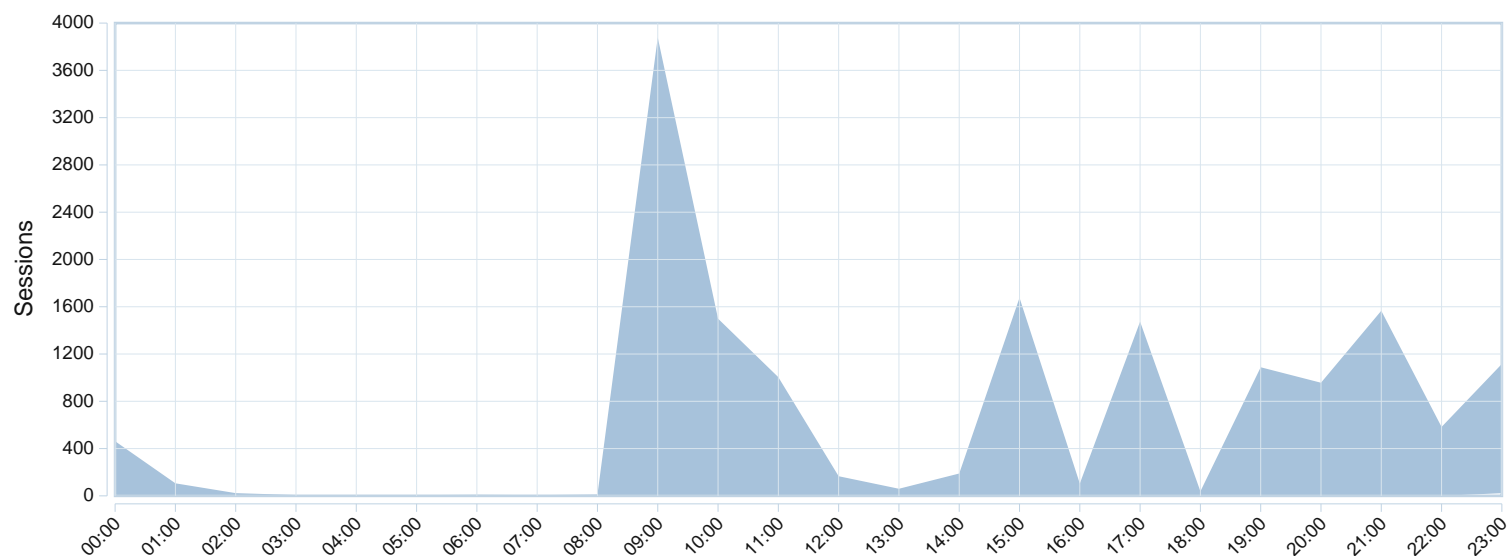
VPN Usage.....	9
Site-to-Site IPSec Tunnels by Bandwidth.....	9
Client-to-Site IPSec Tunnels by Bandwidth.....	9
SSL-VPN Tunnel Users by Bandwidth.....	9
SSL-VPN Web Mode Users by Bandwidth.....	9
Admin Login and System Events.....	10
Admin Login Summary.....	10
List of Failed Logins.....	10
System Events.....	10

Bandwidth and Applications

Bandwidth



Number of Sessions



Traffic Statistics

Summary	Stats
Total Sessions	16.0 K
Total Bytes	In: 4.5 MB Out: 2.4 MB
Average Sessions Per Hour	668
Average Bytes Per Hour	In: 191.9 KB Out: 102.5 KB
Most Active Hour By Sessions	2016-12-30 09:00
Total Users	3
Total Applications	12
Total Destinations	381

Top Applications by Bandwidth

Application	Traffic Out	Traffic In	Sessions
DNS	4.4 MB		13.6 K
HTTPS	1.3 MB		1.3 K
HTTP	1.1 MB		1.2 K
tcp/8081	79.0 KB		18
Yahoo.Mail	25.9 KB		1
Yahoo.Services	13.4 KB		2
HTTPS_7443	9.9 KB		10
Microsoft.Portal	7.1 KB		1
tcp/8080	5.0 KB		8
NTP	988 B		4

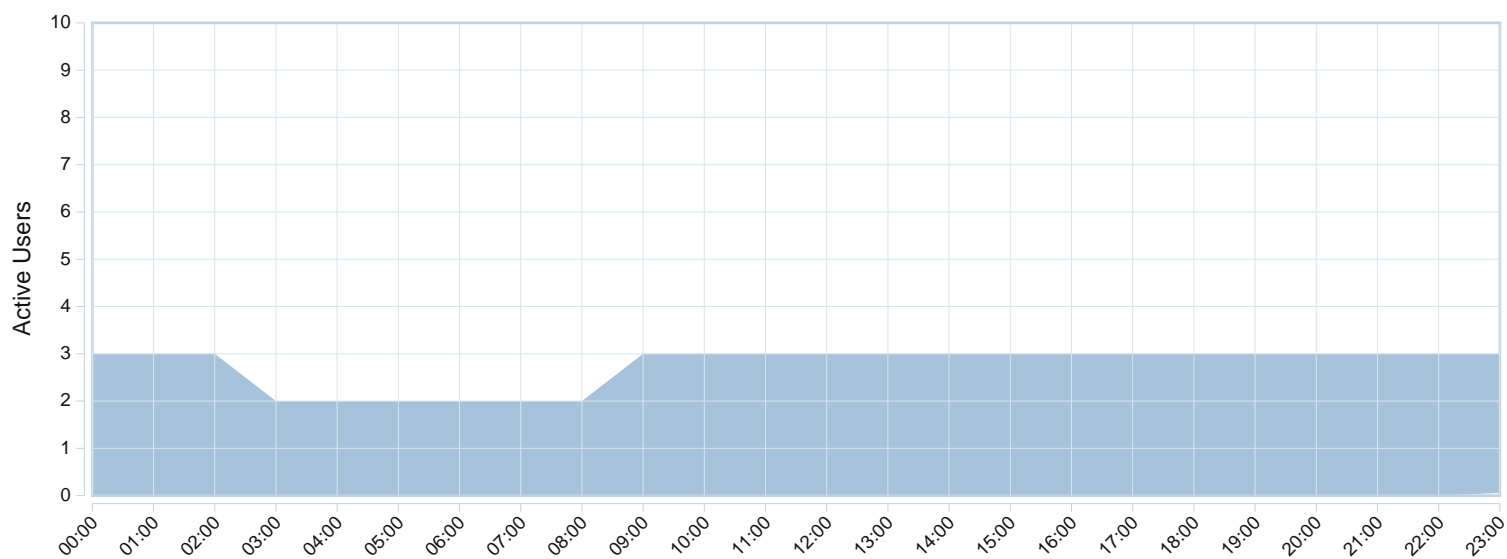
Top Application Categories by Bandwidth

Application Category	Traffic Out	Traffic In	Sessions
unscanned	6.9 MB		16.0 K
Email	25.9 KB		1
General.Interest	13.4 KB		2
Collaboration	7.1 KB		1
Network.Service	1.2 KB		2
Web.Client	370 B		1

Top Users by Bandwidth

User	Host	Traffic Out	Traffic In	Sessions
10.182.8.65	Spare	6.6 MB		15.8 K
172.26.6.66	TIVO-7460001909D8CF9	260.6 KB		171
172.26.6.65	Linksys24449	4.5 KB		24

Number of Active Users



Top Destinations by Bandwidth

Hostname (or IP)	Traffic Out	Traffic In	Sessions
71.170.175.104	3.1 MB		9.8 K
71.170.175.108	1.3 MB		3.8 K
151.101.48.124	228.5 KB		99
204.176.49.116	91.9 KB		26
216.58.194.142	90.1 KB		106
208.73.181.96	78.6 KB		17
52.6.65.143	76.3 KB		53
23.76.195.211	75.3 KB		79
151.101.49.52	70.6 KB		53
216.58.194.131	66.5 KB		68

Web Usage

Top Allowed Websites

Website	Requests
No matching log data for this report	

Top Websites by Bandwidth

Website	Traffic Out	Traffic In
No matching log data for this report		

Top Blocked Websites

Website	Requests
No matching log data for this report	

Top Users by Blocked Requests

User(or IP)	Hostname(MAC)	Requests
No matching log data for this report		

Top Users by Requests

User(or IP)	Hostname(MAC)	Requests
No matching log data for this report		

Top Users by Bandwidth

User(or IP)	Hostname(Mac)	Traffic Out	Traffic In
No matching log data for this report			

Top Video Streaming Web Sites by Bandwidth

No matching log data for this report			
--------------------------------------	--	--	--

Emails

Top Senders by Number of Emails

Sender	Number of Emails
No matching log data for this report	

Top Senders by Combined Email Size

Sender	Bandwidth
No matching log data for this report	

Top Recipients by Number of Emails

Recipient	Number of Emails
No matching log data for this report	

Top Recipients by Combined Email Size

Recipient	Bandwidth
No matching log data for this report	

Threats

Malware Detected

#	Malware Name	Malware Type	Occurrence
No matching log data for this report			

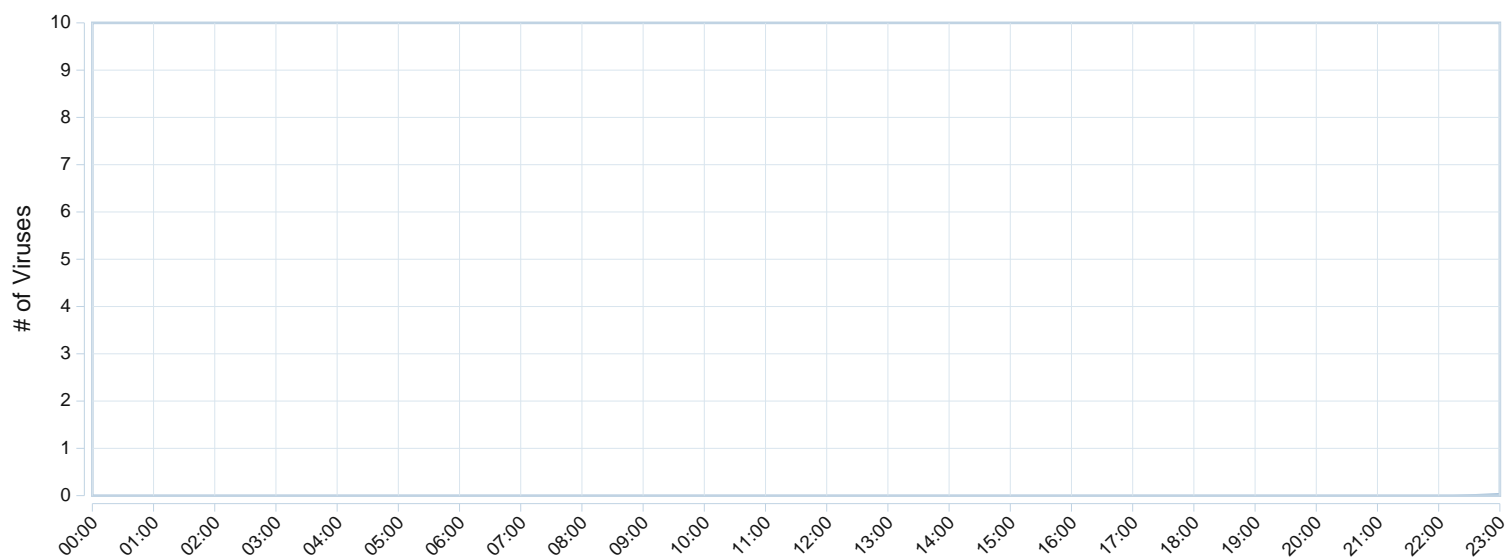
Malware Victims

#	Victim	Occurrence
No matching log data for this report		

Malware Sources

#	Malware Source	Host Name	Counts
No matching log data for this report			

Malware History



Botnet Detected

#	Botnet Name	Counts
No matching log data for this report		

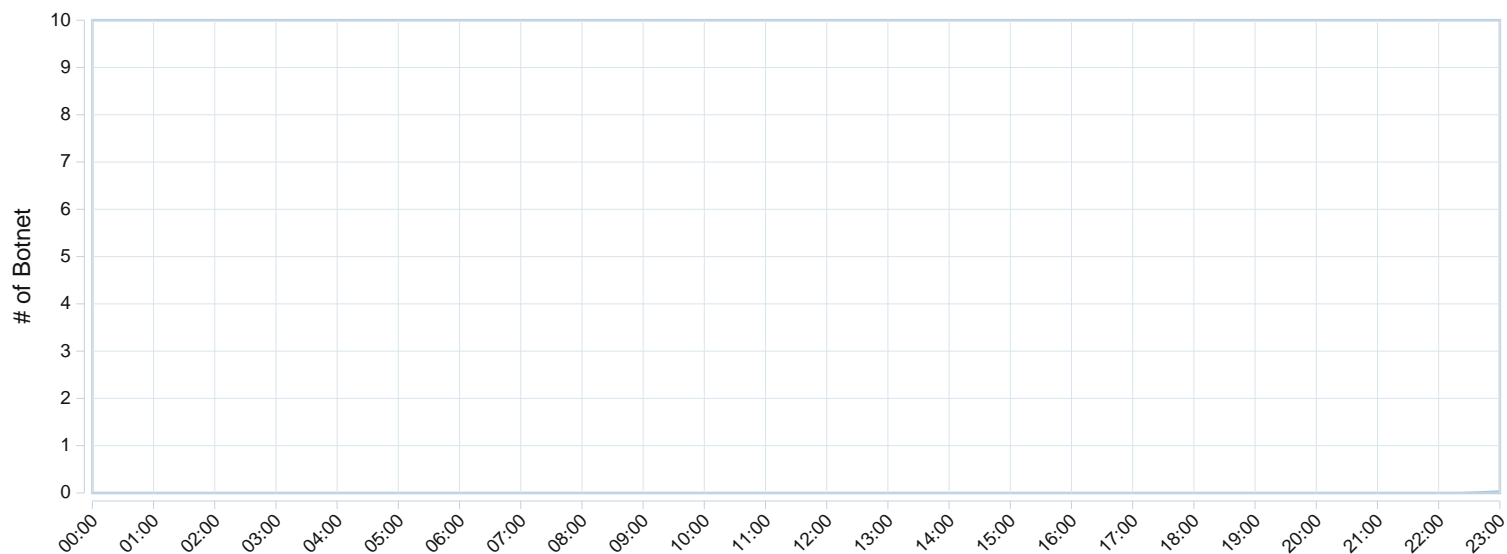
Botnet Victims

#	Victim Name	Counts
No matching log data for this report		

Botnet C&C

#	C & C IP	Host Name	Counts
No matching log data for this report			

Botnet History



Intrusions Detected

#	Intrusion Name	Counts
No matching log data for this report		

Intrusion Victims

#	Intrusion Victim	Counts
No matching log data for this report		

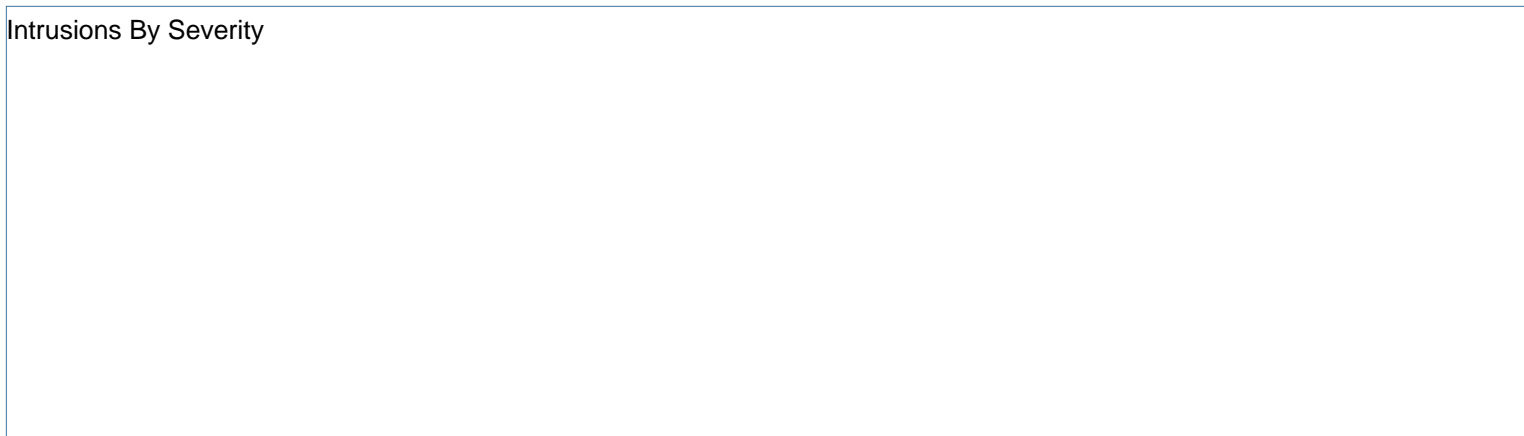
Intrusion Sources

#	Intrusion Source	Counts
No matching log data for this report		

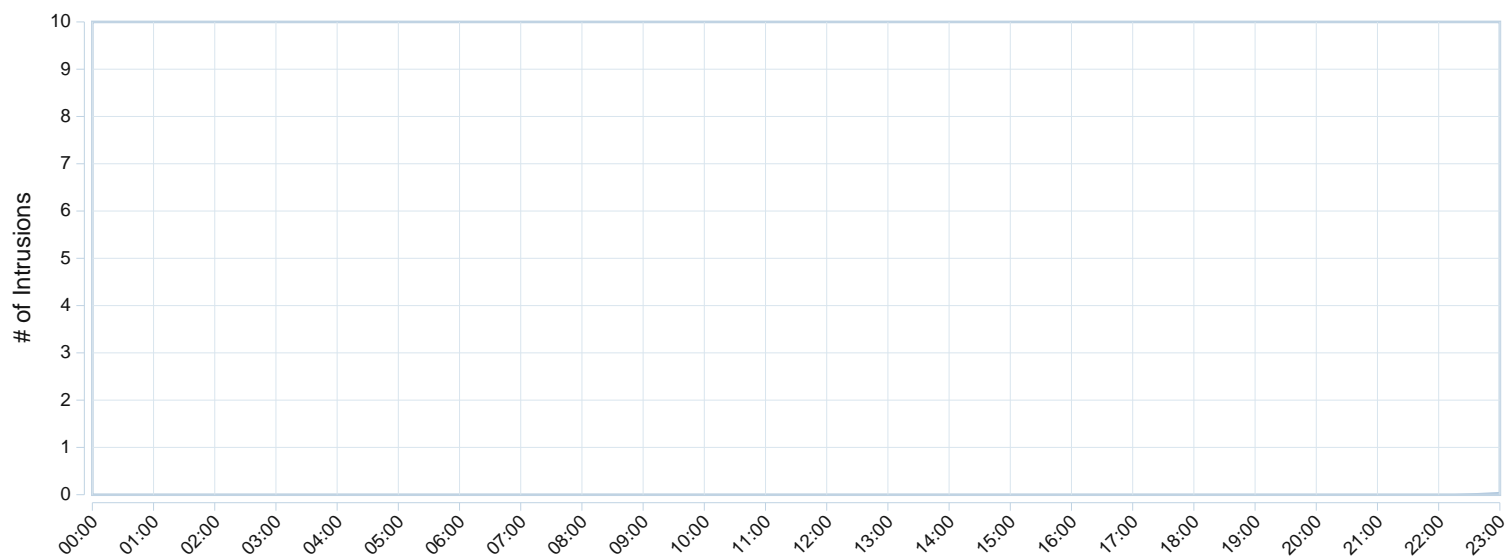
Intrusions Blocked

#	Intrusion Name	Counts
No matching log data for this report		

Intrusions By Severity



Intrusion History



VPN Usage

Site-to-Site IPSec Tunnels by Bandwidth

#	Tunnel	Duration	Traffic Out	Traffic In
No matching log data for this report				

Client-to-Site IPSec Tunnels by Bandwidth

#	User	Tunnel	Duration	Traffic Out	Traffic In
No matching log data for this report					

SSL-VPN Tunnel Users by Bandwidth




#	User	IP	Traffic Out	Traffic In
No matching log data for this report				

SSL-VPN Web Mode Users by Bandwidth

#	User	IP	Traffic Out	Traffic In
No matching log data for this report				

Admin Login and System Events



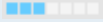
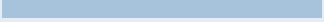
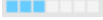

Admin Login Summary

#	User Name	Login Interface	Total # of Logins	Total # of Configuration Changes	Total Duration
1	admin	https(71.170.175.104)	 1	0	15m 20s
2	admin	ssh(71.170.175.104)	 1	 1	11m 06s

List of Failed Logins

#	User Name	Login Interface	# of Failed Logins
No matching log data for this report			

System Events

#	Event Name (Description)	Severity	Counts
1	Configuration changed		 1
2	Interface status changed		 2
3	Disk log file deleted		 1