

FortiGate

# FortiGate Daily Security Report

Report Date: 2023-11-17

Data Range: Nov 16, 2023 (INGO-FG)



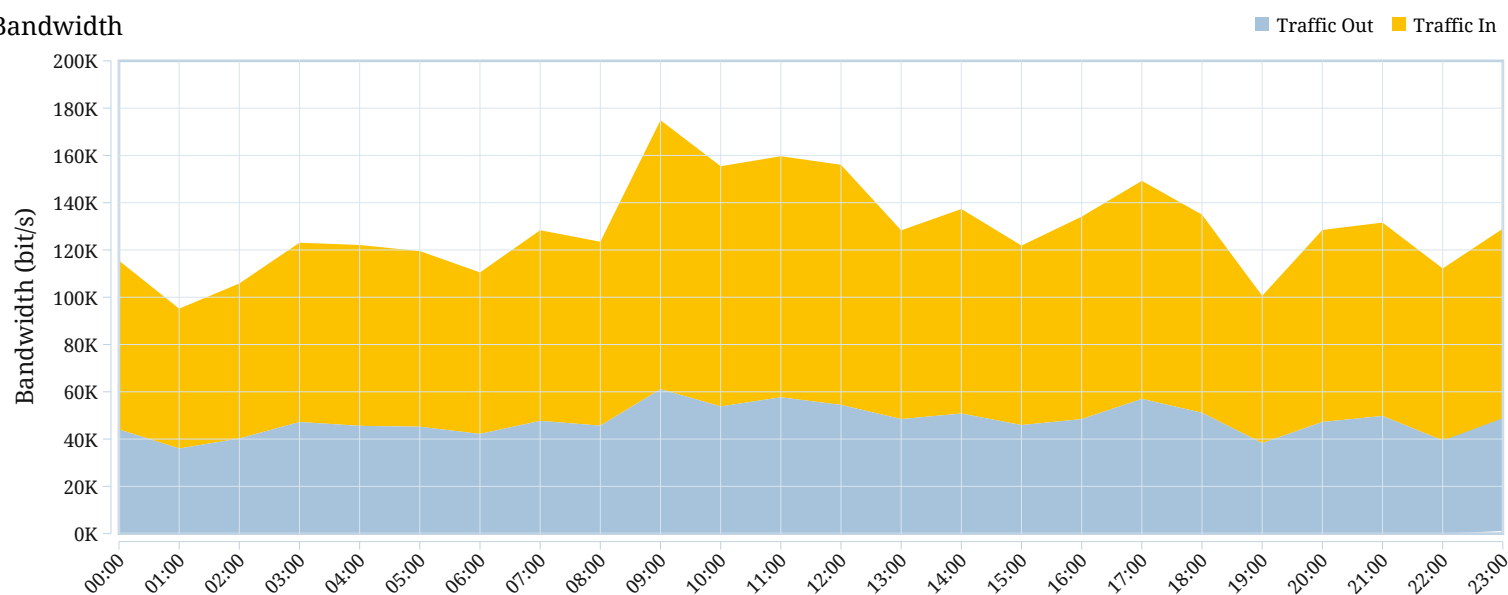
# Table of Contents

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.....	5
Top Users by Bandwidth.....	5
Top Video Streaming Web Sites by Bandwidth.....	6
Emails.....	7
Top Senders by Number of Emails.....	7
Top Senders by Combined Email Size.....	7
Top Recipients by Number of Emails.....	7
Top Recipients by Combined Email Size.....	7
Threats.....	8
Malware Detected.....	8
Malware Victims.....	8
Malware Sources.....	8
Malware History.....	8
Botnet Detected.....	8
Botnet Victims.....	8
Botnet C&C.....	9
Botnet History.....	9
Intrusions Detected.....	9
Intrusion Victims.....	9
Intrusion Sources.....	9
Intrusions Blocked.....	9
Intrusions By Severity.....	10
Intrusion History.....	10

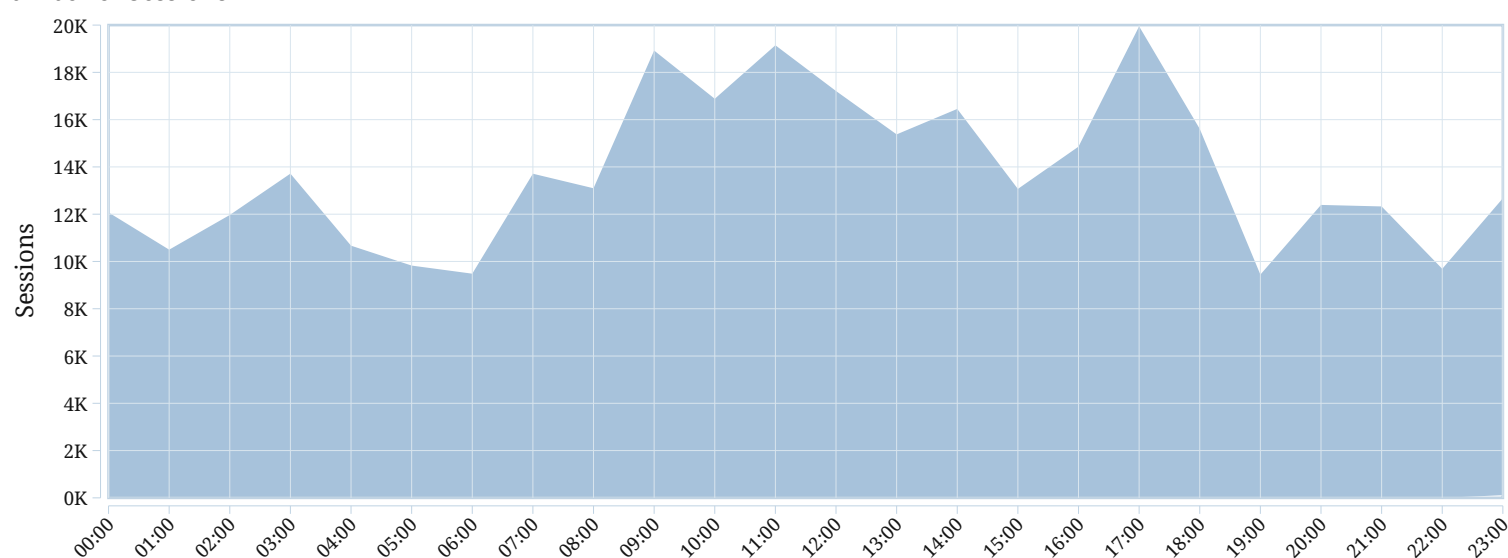
VPN Usage.....	11
Site-to-Site IPSec Tunnels by Bandwidth.....	11
Client-to-Site IPSec Tunnels by Bandwidth.....	11
SSL-VPN Tunnel Users by Bandwidth.....	11
SSL-VPN Web Mode Users by Bandwidth.....	11
Admin Login and System Events.....	12
Admin Login Summary.....	12
List of Failed Logins.....	12
System Events.....	12

# Bandwidth and Applications

Bandwidth



Number of Sessions



## Traffic Statistics

Summary	Stats
Total Sessions	329.0 K
Total Bytes	In: 837.2 MB Out: 491.9 MB
Average Sessions Per Hour	13.7 K
Average Bytes Per Hour	In: 34.9 MB Out: 20.5 MB
Most Active Hour By Sessions	2023-11-16 17:00
Total Users	1.1 K
Total Applications	7
Total Destinations	69

## Top Applications by Bandwidth

Application	Traffic Out	Traffic In	Sessions
HTTPS		687.5 MB	99.0 K
HTTP		641.7 MB	230.1 K
MMS		11.0 KB	1
udp/443		8.8 KB	1
tcp/6568		2.3 KB	4
tcp/8908		672 B	3
tcp/3738		164 B	1

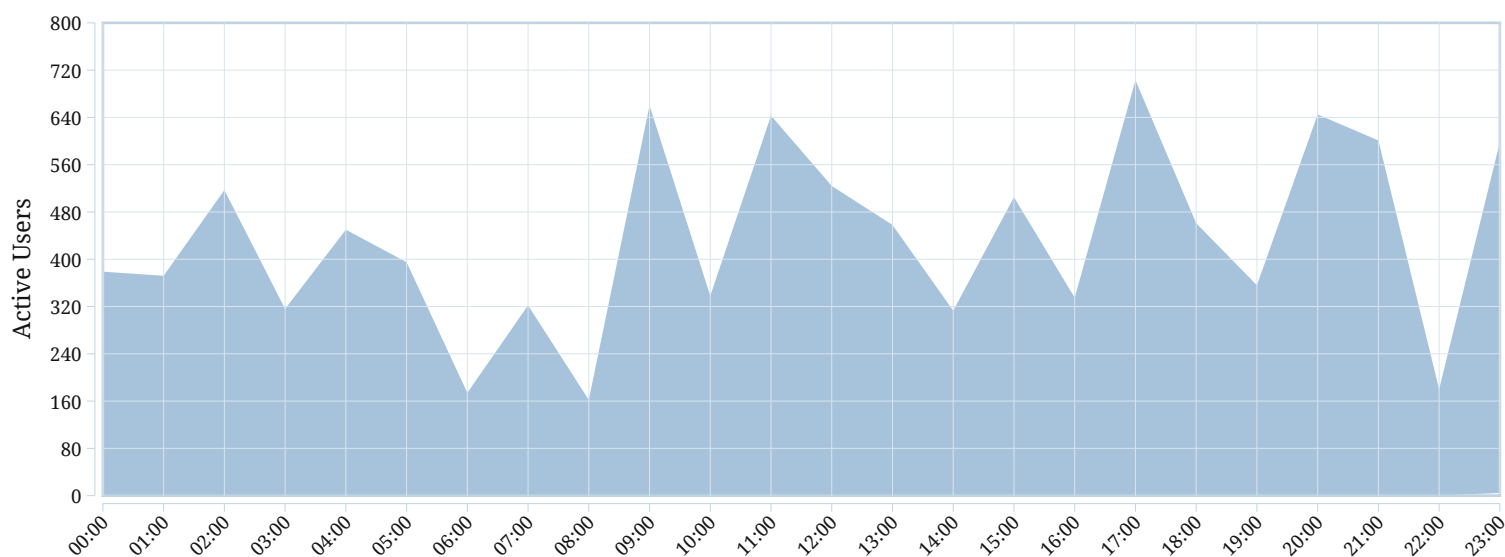
## Top Application Categories by Bandwidth

Application Category	Traffic Out	Traffic In	Sessions
unscanned		1.3 GB	329.0 K

## Top Users by Bandwidth

User	Host	Traffic Out	Traffic In	Sessions
185.213.229.194	185.213.229.194		8.7 MB	146
192.168.4.35	192.168.4.35		6.5 MB	38
213.230.74.161	213.230.74.161		5.4 MB	53
213.180.203.126	213.180.203.126		5.4 MB	914
95.108.213.89	95.108.213.89		5.1 MB	863
213.180.203.32	213.180.203.32		4.8 MB	803
192.168.4.46	192.168.4.46		4.8 MB	122
213.180.203.195	213.180.203.195		4.7 MB	831
5.255.231.39	5.255.231.39		4.5 MB	1.0 K
87.250.224.53	87.250.224.53		4.5 MB	889

## Number of Active Users



## Top Destinations by Bandwidth

Hostname (or IP)	Traffic Out	Traffic In	Sessions
192.168.4.192		1.3 GB	328.5 K
18.142.196.21		49.7 KB	24
54.254.188.33		46.5 KB	26
apple.com		26.9 KB	8
mail.ru		15.6 KB	53
e-otsenka.uz		14.3 KB	23
149.154.167.41		12.5 KB	12
uniqueduty.com		12.4 KB	9
149.154.167.255		12.3 KB	9
17.188.179.25		11.0 KB	1

## Web Usage

### Top Allowed Websites

Website	Requests
apple.com	8
icloud.com	3
assistances.info	2
185.229.191.44	2
5.189.202.18	1











### Top Websites by Bandwidth

Website	Traffic Out	Traffic In	
18.142.196.21			49.7 KB
54.254.188.33			46.5 KB
apple.com			25.1 KB
mail.ru			15.6 KB
e-otsenka.uz			14.3 KB
149.154.167.41			12.5 KB
uniqueduty.com			12.4 KB
149.154.167.255			12.3 KB
windowsupdate.com			10.3 KB
tashkent.delivery			10.2 KB

### Top Blocked Websites

Website	Requests
mail.ru	53
spaceneobank.com	27
korzinka-application.uz	26
54.254.188.33	26
18.142.196.21	24
e-otsenka.uz	23
rfihub.com	22
browworkers5s.com	17
scpvnth.xyz	14
google.com	14

### Top Users by Blocked Requests

User(or IP)	Hostname(MAC)	Requests
 192.168.4.10	 192.168.4.10	62
 192.168.4.110	 192.168.4.110	52
 192.168.4.49	 192.168.4.49	50
 192.168.4.115	 192.168.4.115	47
 192.168.4.45	 192.168.4.45	25

## Top Users by Blocked Requests (contd)

User(or IP)	Hostname(MAC)	Requests
192.168.4.48	192.168.4.48	17
192.168.4.81	192.168.4.81	17
192.168.4.85	192.168.4.85	15
192.168.4.105	192.168.4.105	14
192.168.4.52	192.168.4.52	13

## Top Users by Requests

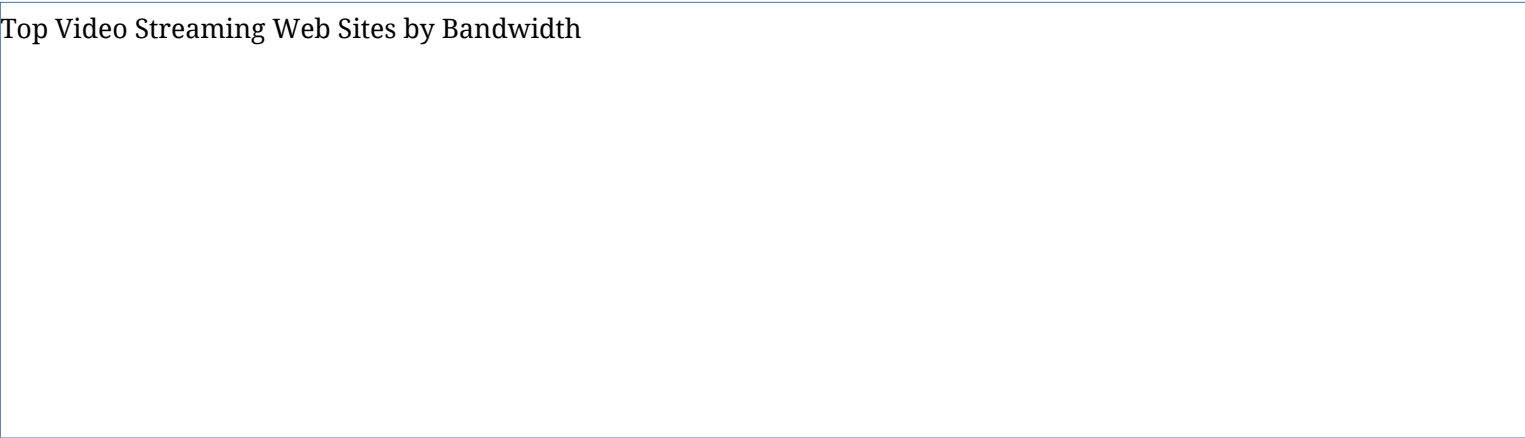
User(or IP)	Hostname(MAC)	Requests
192.168.4.10	192.168.4.10	71
192.168.4.110	192.168.4.110	52
192.168.4.49	192.168.4.49	52
192.168.4.115	192.168.4.115	47
192.168.4.45	192.168.4.45	25
192.168.4.48	192.168.4.48	17
192.168.4.81	192.168.4.81	17
192.168.4.105	192.168.4.105	15
192.168.4.85	192.168.4.85	15
192.168.4.150	192.168.4.150	14
Average Usage of Top 10		32

## Top Users by Bandwidth

User(or IP)	Hostname(Mac)	Traffic Out	Traffic In
192.168.4.110	192.168.4.110		
192.168.4.10	192.168.4.10		
192.168.4.49	192.168.4.49		
192.168.4.45	192.168.4.45		
192.168.4.150	192.168.4.150		
192.168.4.115	192.168.4.115		
192.168.4.31	192.168.4.31		
192.168.4.61	192.168.4.61		
192.168.4.52	192.168.4.52		
192.168.4.105	192.168.4.105		
Average Usage of Top 10			



Top Video Streaming Web Sites by Bandwidth



## 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			

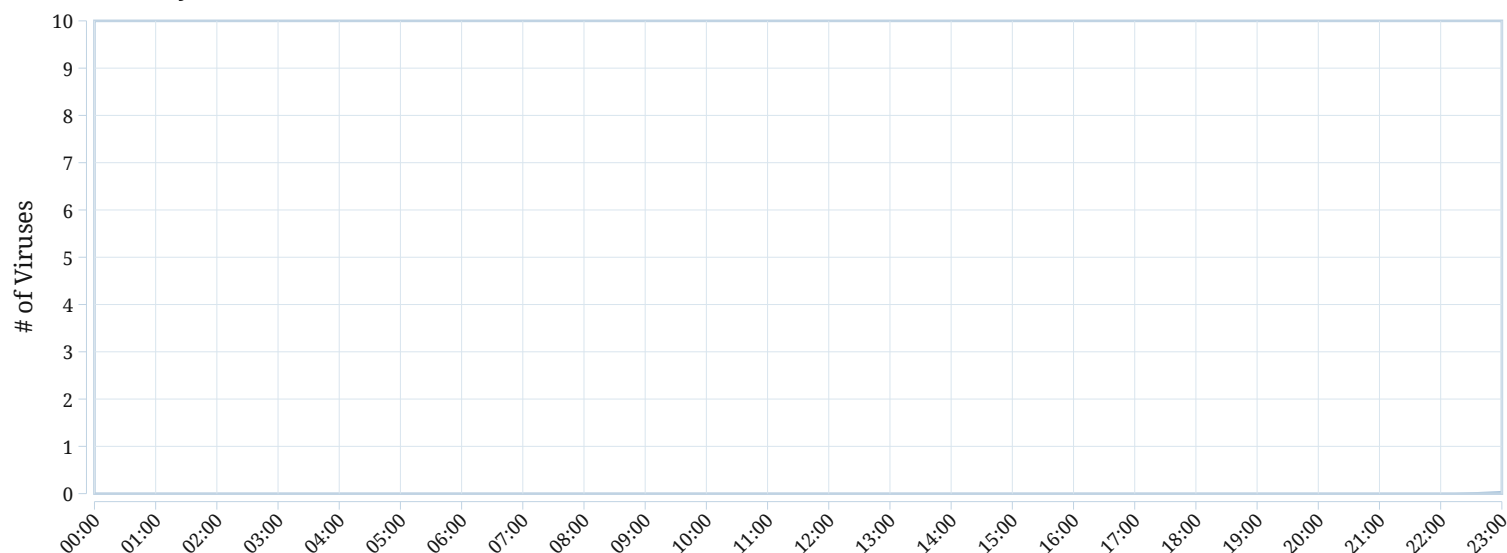
## Malware Victims

#	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		

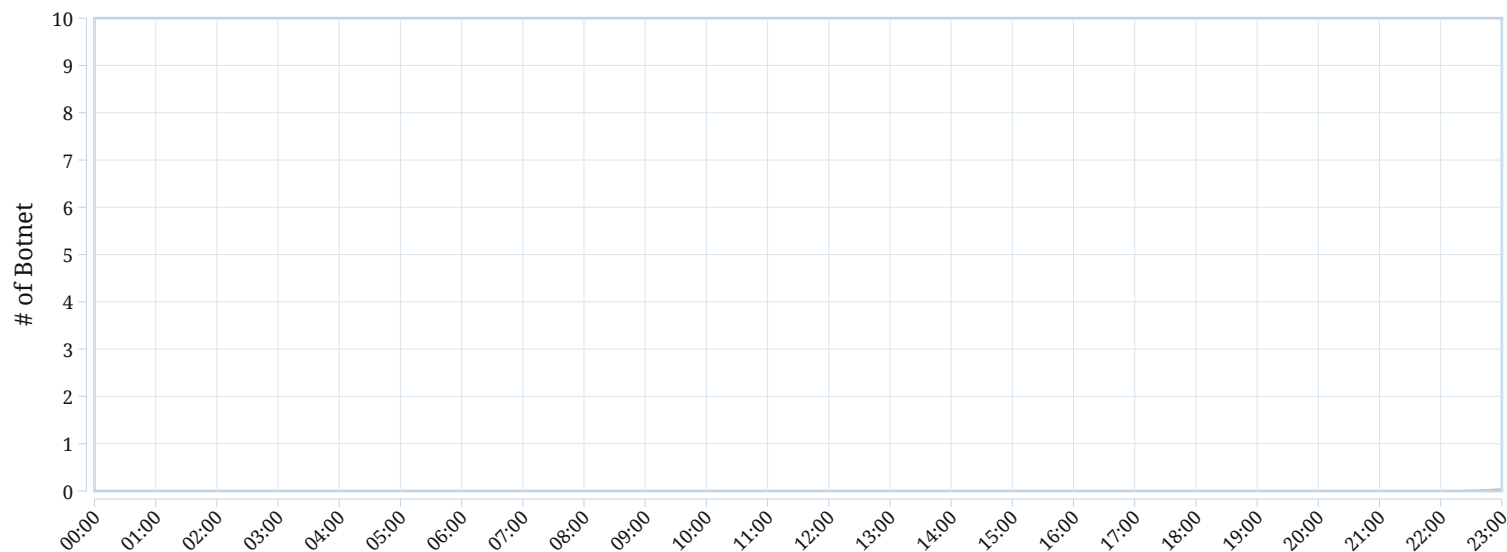
## Botnet Victims

#	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		

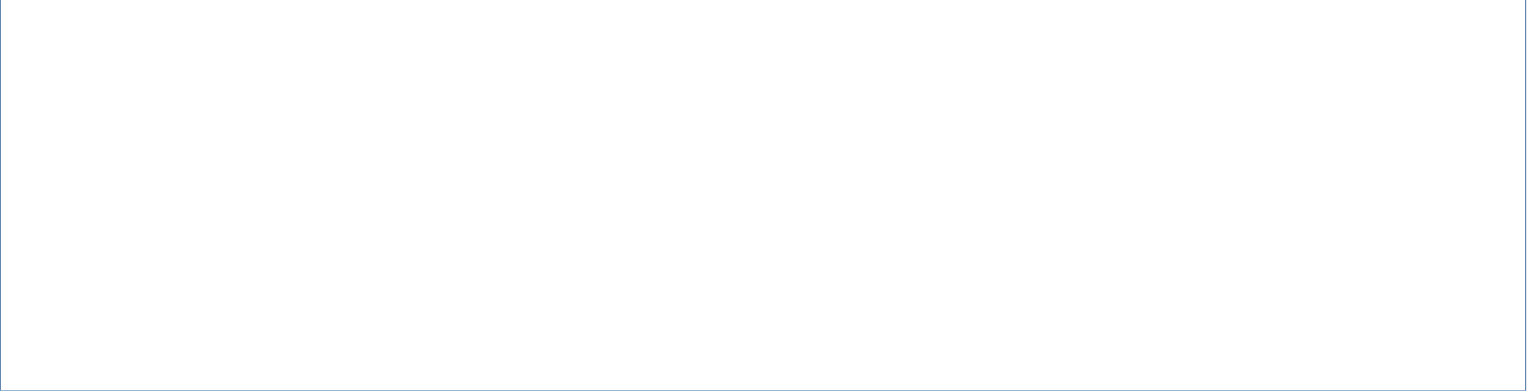
## Intrusion Sources

#	Intrusion Source	Counts
No matching log data for this report		

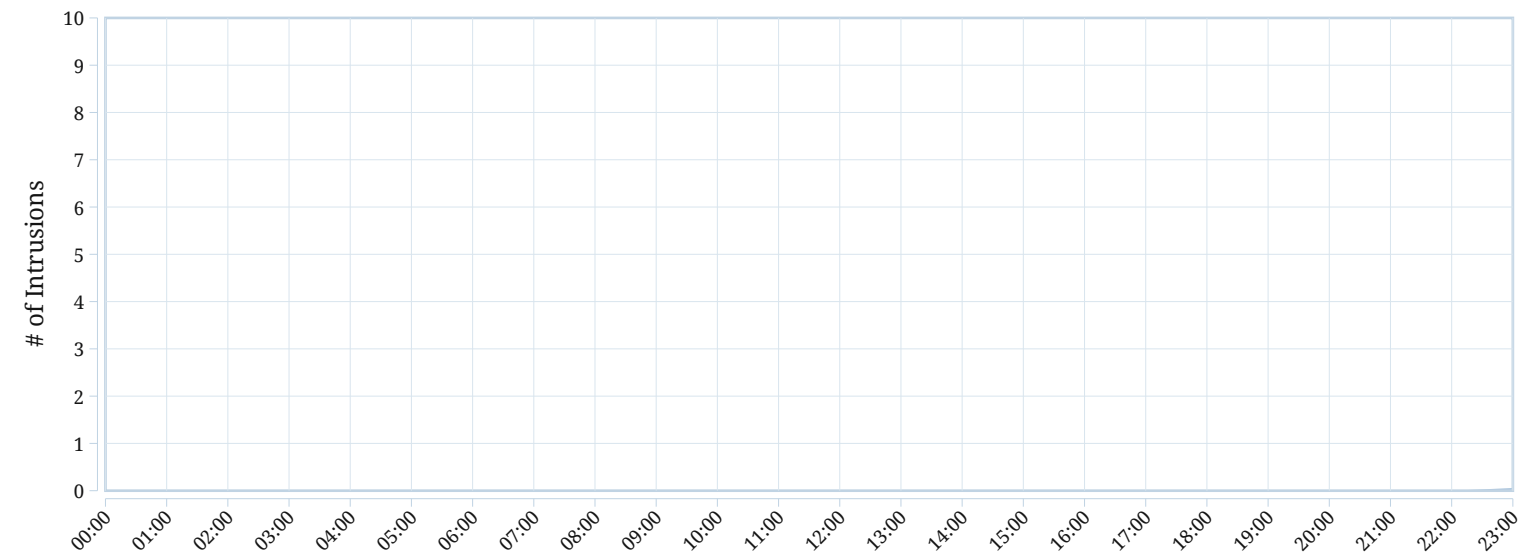
## Intrusions Blocked

#	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	XAuther 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(192.168.4.45)	<div><div></div></div> 2	0	02h 05m 52s

### 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	Disk scan is needed	<div><div></div></div>	<div><div></div></div> 1
2	Device rebooted	<div><div></div></div>	<div><div></div></div> 1
3	Format disk requested	<div><div></div></div>	<div><div></div></div> 1
4	URL filter packet send failure	<div><div></div></div>	<div><div></div></div> 1
5	Interface status changed	<div><div></div></div>	<div><div></div></div> 9
6	Central Management connectivity is inactive	<div><div></div></div>	<div><div></div></div> 4
7	Disk log file deleted	<div><div></div></div>	<div><div></div></div> 4
8	Clear active sessions	<div><div></div></div>	<div><div></div></div> 2
9	Optional power supply not detected	<div><div></div></div>	<div><div></div></div> 1