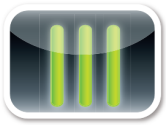


FortiGate

FortiGate Daily Security Report

Report Date: 2022-02-22

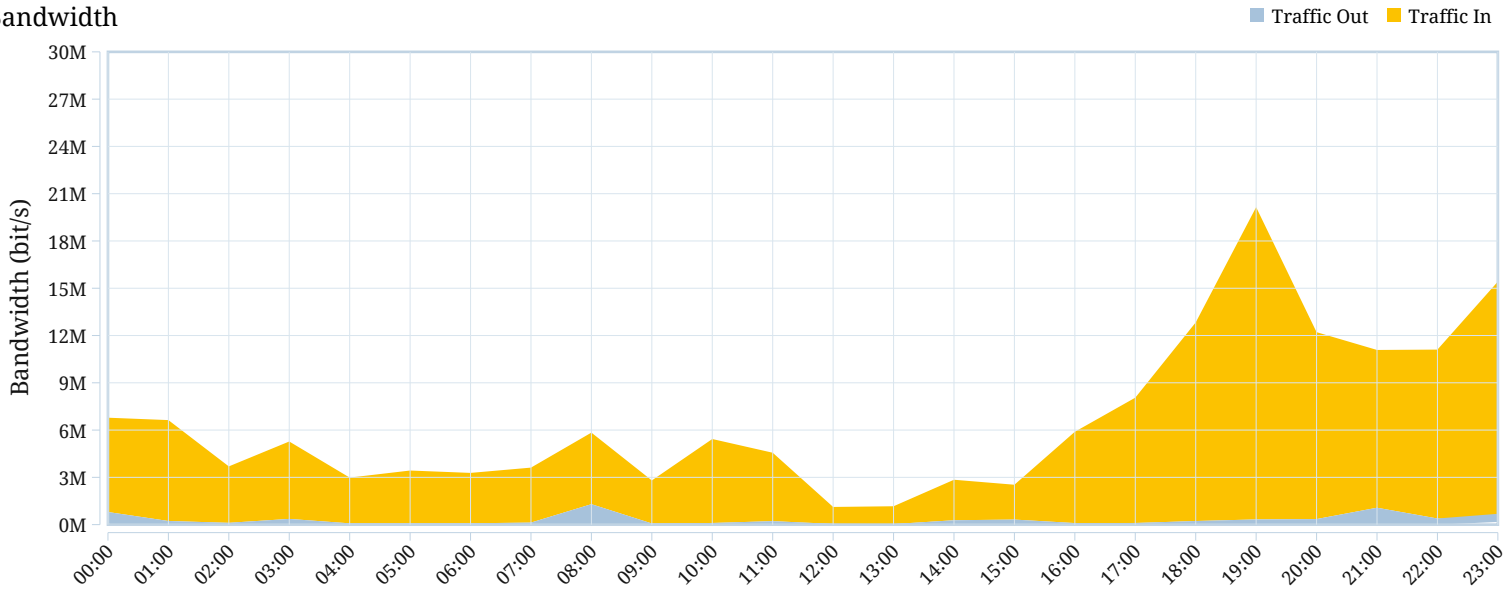
Data Range: Feb 21, 2022 (FortiGate-61F)

FORTINET

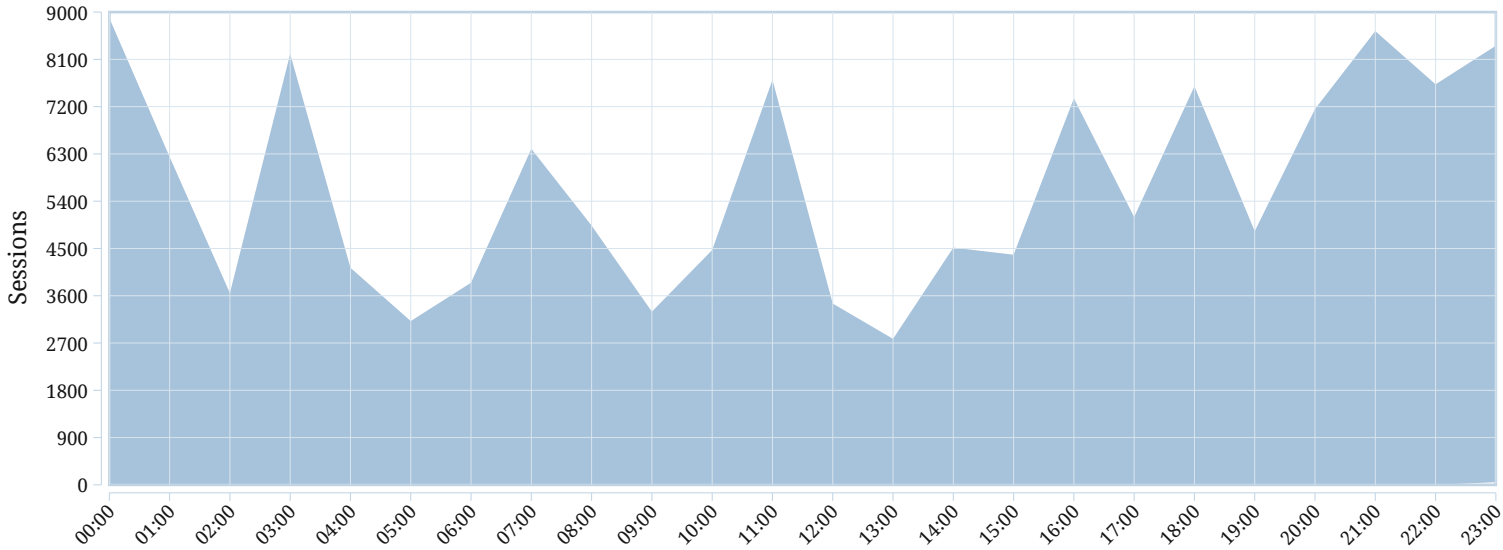
Table of Contents

Bandwidth and Applications

Bandwidth



Number of Sessions



Traffic Statistics

Summary	Stats
Total Sessions	136.7 K
Total Bytes	In: 63.4 GB Out: 3.2 GB
Average Sessions Per Hour	5.7 K
Average Bytes Per Hour	In: 2.6 GB Out: 134.6 MB
Most Active Hour By Sessions	2022-02-21 00:00
Total Users	77
Total Applications	197
Total Destinations	2.8 K

Top Applications by Bandwidth

Application	Traffic Out / Traffic In	Sessions
QUIC	27.4 GB	12.9 K
Netflix	17.8 GB	1.7 K
HTTPS.BROWSER	5.2 GB	15.3 K
YouTube	3.5 GB	3.7 K
Apple.Services	2.6 GB	2.7 K
Apple.Store	2.4 GB	1.5 K
STUN	2.1 GB	36
Facebook	1.7 GB	3.8 K
Naver.Line	1.2 GB	2.8 K
Google.Hangouts	597.8 MB	27

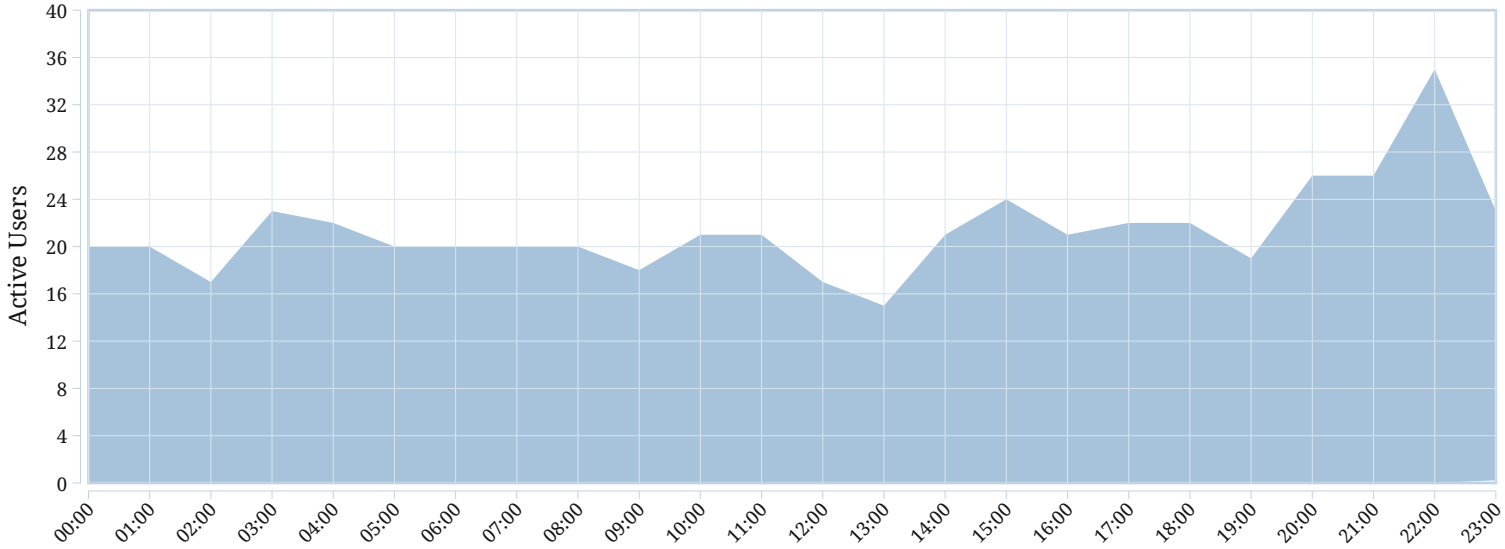
Top Application Categories by Bandwidth

Application Category	Traffic Out / Traffic In	Sessions
Network.Service	29.6 GB	78.6 K
Video/Audio	22.1 GB	5.9 K
General.Interest	5.4 GB	10.9 K
Web.Client	5.3 GB	17.0 K
Collaboration	1.9 GB	5.6 K
Social.Media	1.1 GB	4.1 K
unscanned	446.6 MB	3.5 K
Storage.Backup	308.9 MB	2.6 K
Update	210.3 MB	1.5 K
unknown	132.9 MB	5.1 K

Top Users by Bandwidth

User	Host	Traffic Out / Traffic In	Sessions
10.37.60.112	88dc830d-0688-0d45-0789-c62de	15.2 GB	4.8 K
10.37.12.117	LAPTOP-DJTPU9HC	12.3 GB	2.9 K
10.37.10.111	LAPTOP-Q82QV4AO	11.4 GB	6.9 K
10.37.60.115	96:8c:21:a2:c8:05	4.8 GB	24.1 K
10.37.12.111	DESKTOP-96366GR	3.9 GB	8.2 K
10.37.14.111	DingDing	3.6 GB	5.1 K
10.37.60.113	iPhone-2	2.7 GB	14.0 K
10.37.12.118	fa:73:00:73:11:54	2.6 GB	10.8 K
10.37.57.112	Shady-2	1.8 GB	1.4 K
10.37.57.117	chikarahiroshi	1.5 GB	8.7 K

Number of Active Users



Top Destinations by Bandwidth

Hostname (or IP)	Traffic Out / Traffic In	Sessions
nflxvideo.net	17.7 GB	554
203.66.155.178	5.7 GB	12
203.66.155.208	5.1 GB	92
203.66.155.175	3.8 GB	19
googlevideo.com	3.4 GB	1.2 K
cdn-apple.com	2.6 GB	269
apple.com	2.4 GB	5.4 K
203.66.155.141	2.2 GB	6
bytetos.com	2.2 GB	28
39.9.199.204	2.1 GB	8

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

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			

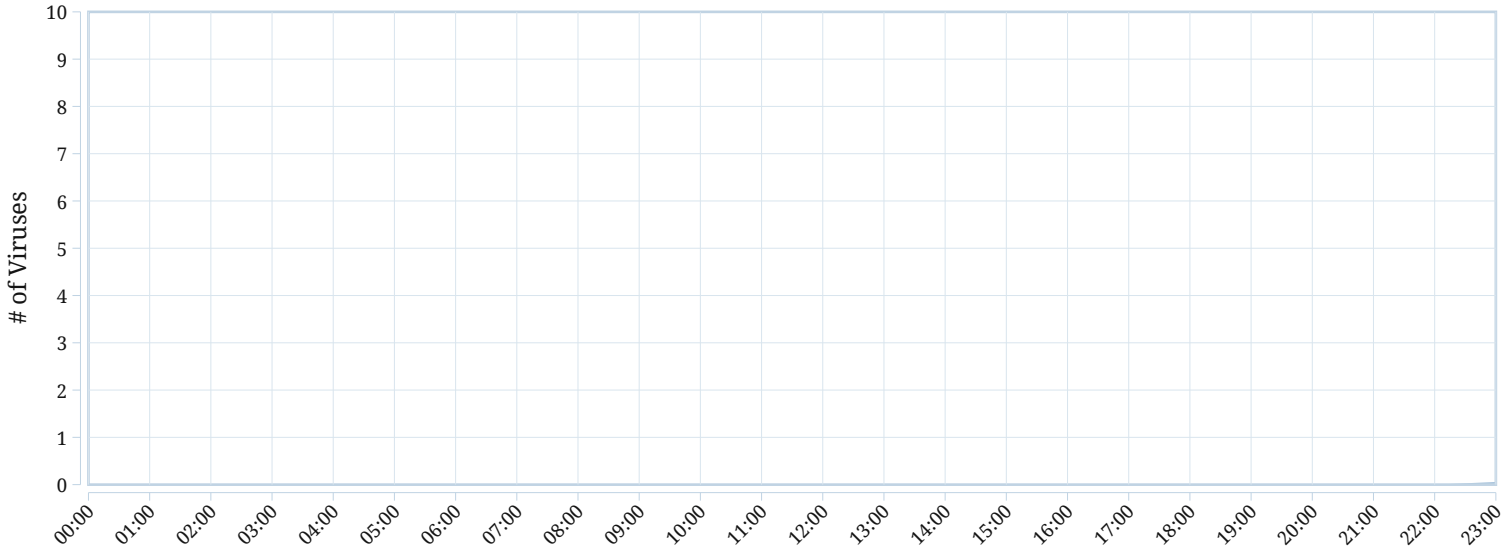
Malware Victims

#	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		

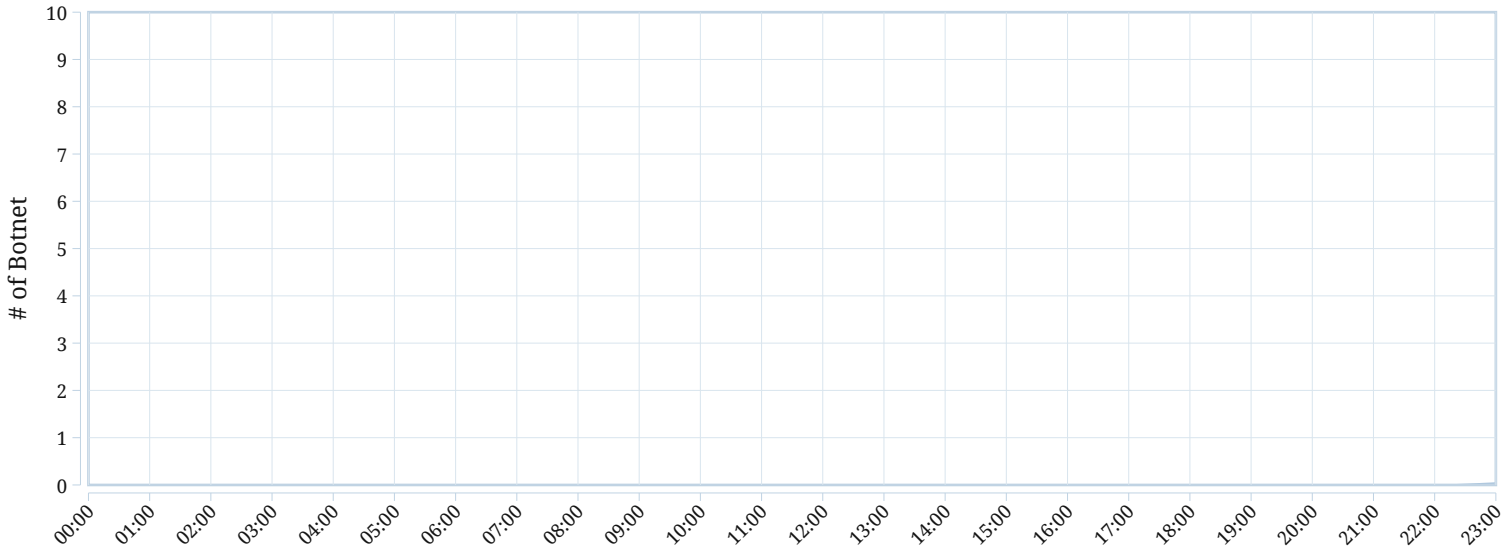
Botnet Victims

#	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

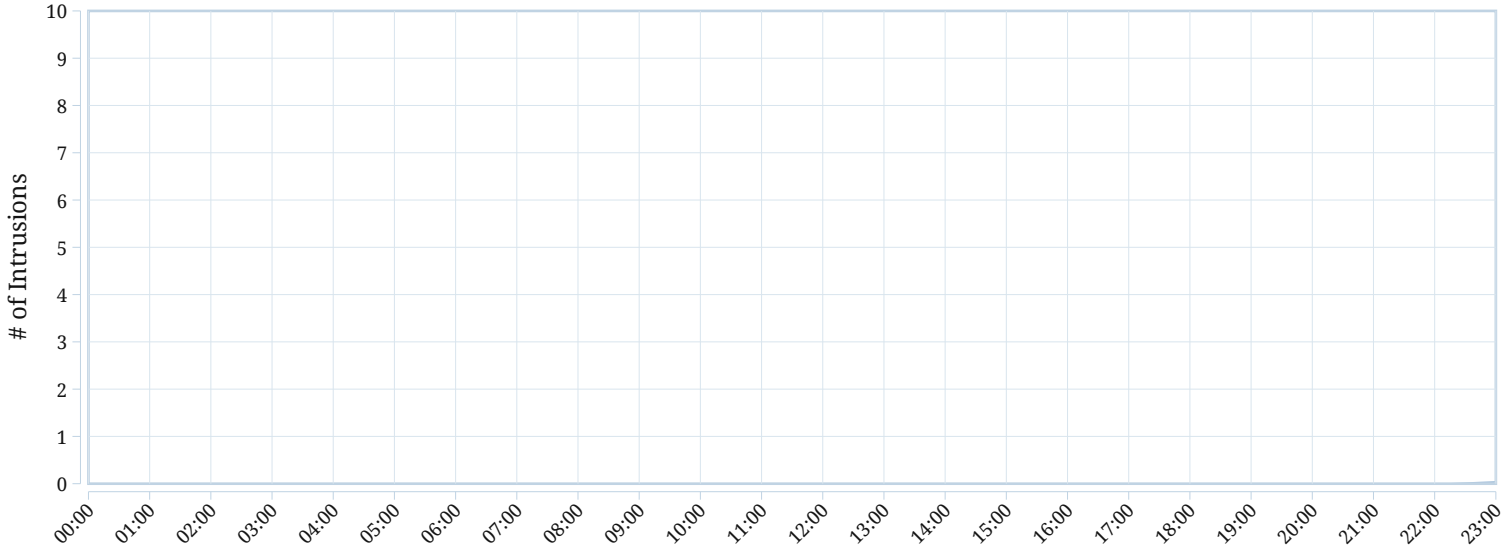
#	Intrusion Source	Counts
No matching log data for this report		

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
No matching log data for this report					

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	FortiCloud activation failed		143
2	Clear active sessions		4
3	Disk log file deleted		1