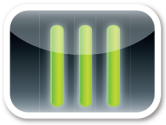


FortiGate

FortiGate Daily Security Report

Report Date: 2019-09-18

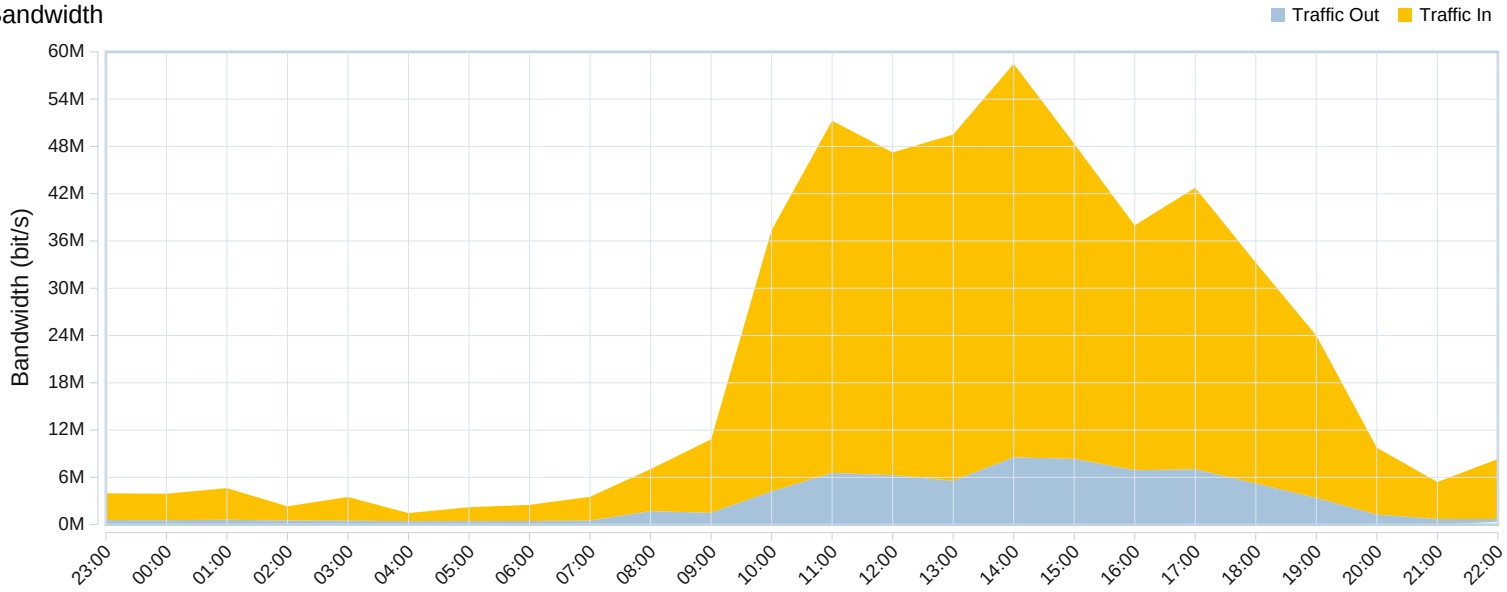
Data Range: 2019-09-16 23:30 -- 2019-09-17 23:29 GMT+5:30 (AINKOLB0000FW01)

FORTINET

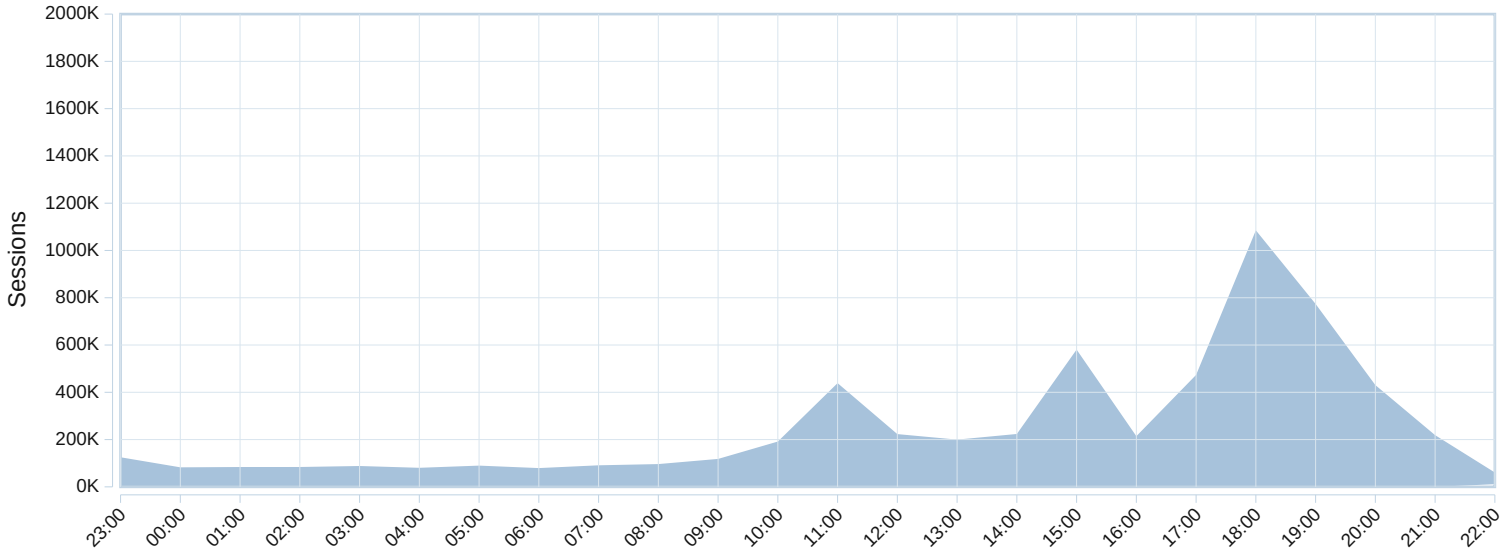
Table of Contents

Bandwidth and Applications

Bandwidth



Number of Sessions



Traffic Statistics

Summary	Stats
Total Sessions	6.1 M
Total Bytes	In: 179.0 GB Out: 30.4 GB
Average Sessions Per Hour	255.6 K
Average Bytes Per Hour	In: 7.5 GB Out: 1.3 GB
Most Active Hour By Sessions	2019-09-17 18:00
Total Users	6.2 K
Total Applications	5.5 K
Total Destinations	10.8 K

Top Applications by Bandwidth

Application	Traffic Out / Traffic In	Sessions
HTTPS	155.7 GB	2.0 M
HTTP	44.6 GB	165.1 K
CDS-58024-60999-UDP	2.9 GB	176
CDS-1433-TCP	756.5 MB	1.1 K
CDS-52000-52999-UDP	605.0 MB	76
udp/54612	566.6 MB	1
udp/55028	432.1 MB	1
udp/57336	386.8 MB	1
udp/56976	287.4 MB	1
udp/54692	281.7 MB	2

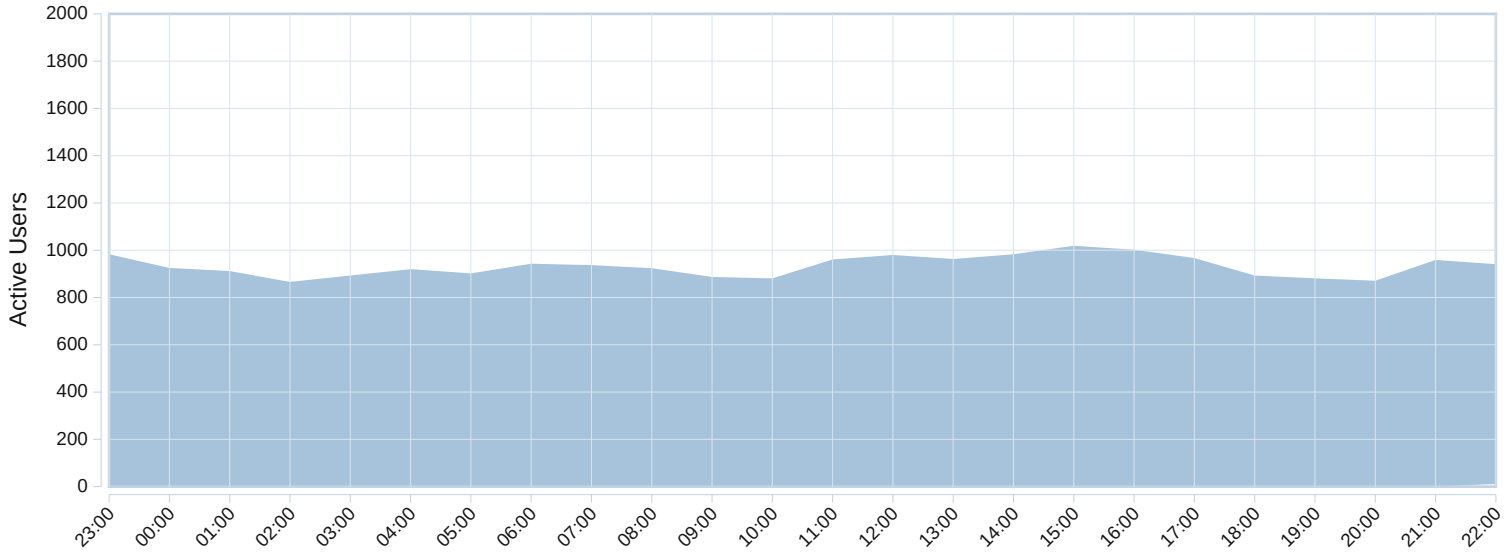
Top Application Categories by Bandwidth

Application Category	Traffic Out / Traffic In	Sessions
unscanned	209.4 GB	5.8 M

Top Users by Bandwidth

User	Host	Traffic Out / Traffic In	Sessions
10.195.25.171	10.195.25.171	13.5 GB	6.7 K
10.195.7.248	10.195.7.248	11.3 GB	2.2 K
10.195.7.191	10.195.7.191	4.7 GB	2.3 K
10.195.25.172	10.195.25.172	4.4 GB	2.9 K
10.195.7.225	10.195.7.225	3.5 GB	817
10.195.25.237	10.195.25.237	3.4 GB	7.1 K
10.195.7.115	10.195.7.115	3.0 GB	2.6 K
10.195.7.142	10.195.7.142	2.7 GB	4.5 K
10.195.25.204	10.195.25.204	2.6 GB	5.6 K
10.195.3.96	10.195.3.96	2.3 GB	2.3 K

Number of Active Users



Top Destinations by Bandwidth

Hostname (or IP)	Traffic Out / Traffic In		Sessions
40.83.104.208		30.9 GB	127
13.107.136.9		13.7 GB	86.4 K
72.21.81.240		5.7 GB	8.2 K
52.113.194.131		4.5 GB	57.9 K
14.139.62.20		4.5 GB	2
93.184.215.201		3.6 GB	502
157.240.15.17		3.5 GB	1.1 K
204.79.197.223		3.1 GB	150
205.185.216.42		3.0 GB	3.4 K
157.240.15.22		3.0 GB	2.3 K

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
1	Malware_Generic.P0	Virus	36
2	JS/Redirector.DN!tr	Virus	10
3	JS/Agent.SZC!tr	Virus	6

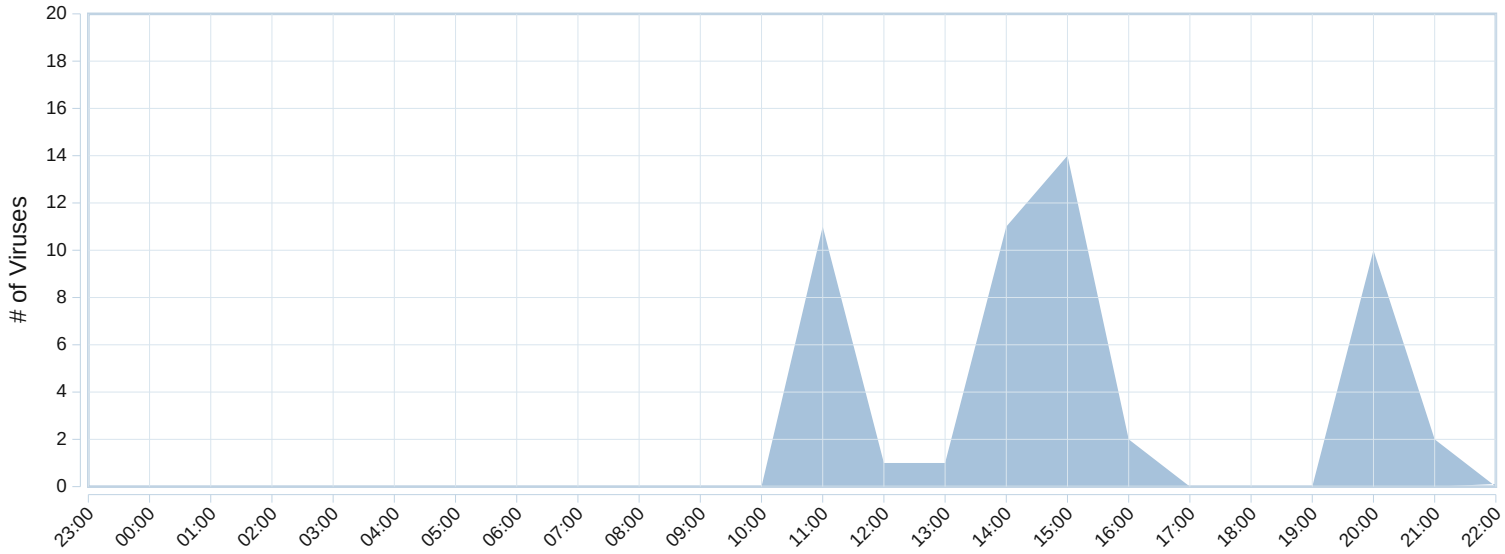
Malware Victims

#	Victim	Occurrence
1	10.195.13.71	36
2	10.195.25.218	10
3	10.195.7.62	6

Malware Sources

#	Malware Source	Host Name	Counts
1	103.83.192.127	103.83.192.127	10
2	13.224.197.131	13.224.197.131	6
3	166.62.72.100	166.62.72.100	6
4	13.225.63.221	13.225.63.221	5
5	52.222.168.46	52.222.168.46	5
6	13.225.218.211	13.225.218.211	4
7	13.225.218.26	13.225.218.26	4
8	13.225.218.137	13.225.218.137	3
9	13.225.218.61	13.225.218.61	2
10	13.225.84.121	13.225.84.121	2
11	13.225.84.177	13.225.84.177	2
12	143.204.178.227	143.204.178.227	1
13	143.204.98.167	143.204.98.167	1
14	52.222.168.104	52.222.168.104	1

Malware History



Botnet Detected

#	Botnet Name	Counts
No matching log data for this report		

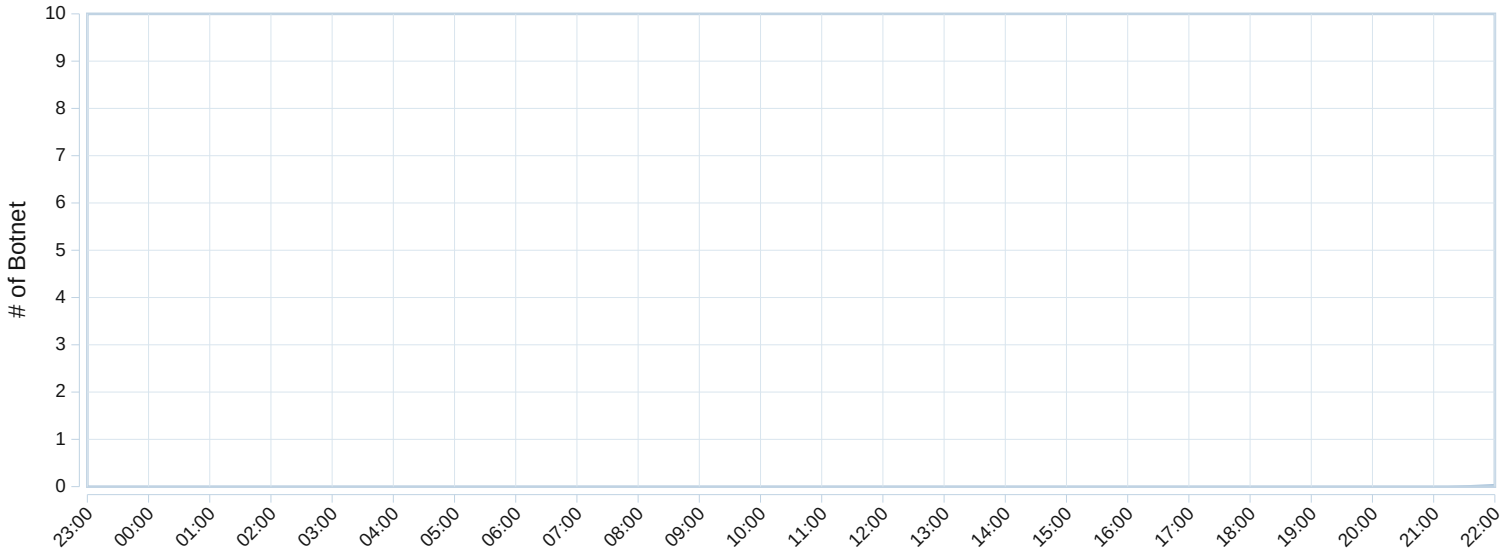
Botnet Victims

#	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

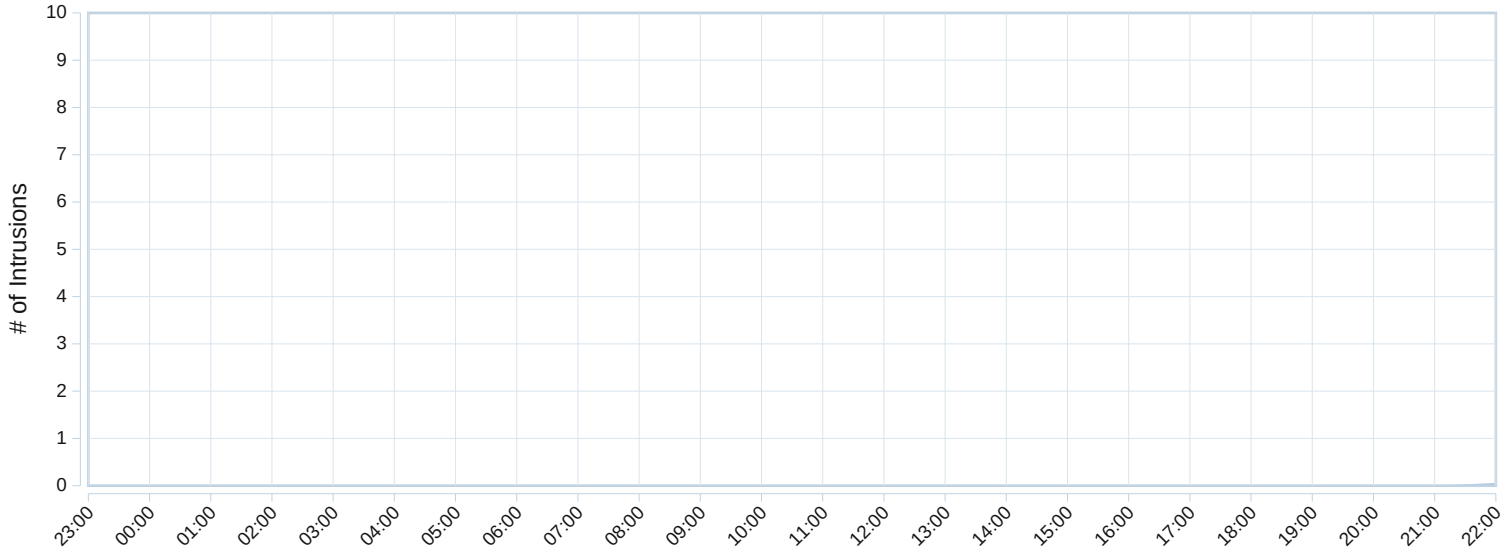
#	Intrusion Source	Counts
No matching log data for this report		

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	jnandi	https(10.195.25.106)	2	0	04h 14m 12s
2	jnandi	https(10.195.0.111)	1	0	03h 05m 36s

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 log file deleted		18
2	SNMP query failed		11