FortiAnalyzer Report

Report Name: Network_Analysis-2011-12-10-2009
Generated on: Sat Dec 10 20:10:26 2011
Scheduled Period: 2011-01-01 00:00 - 2011-12-10 20:09 GMT (FortiAnalyzer local)
Devices: FG110C, FWF60C, FortiVoice, Fortigate-VM_FGVM020000001140
Filters: None

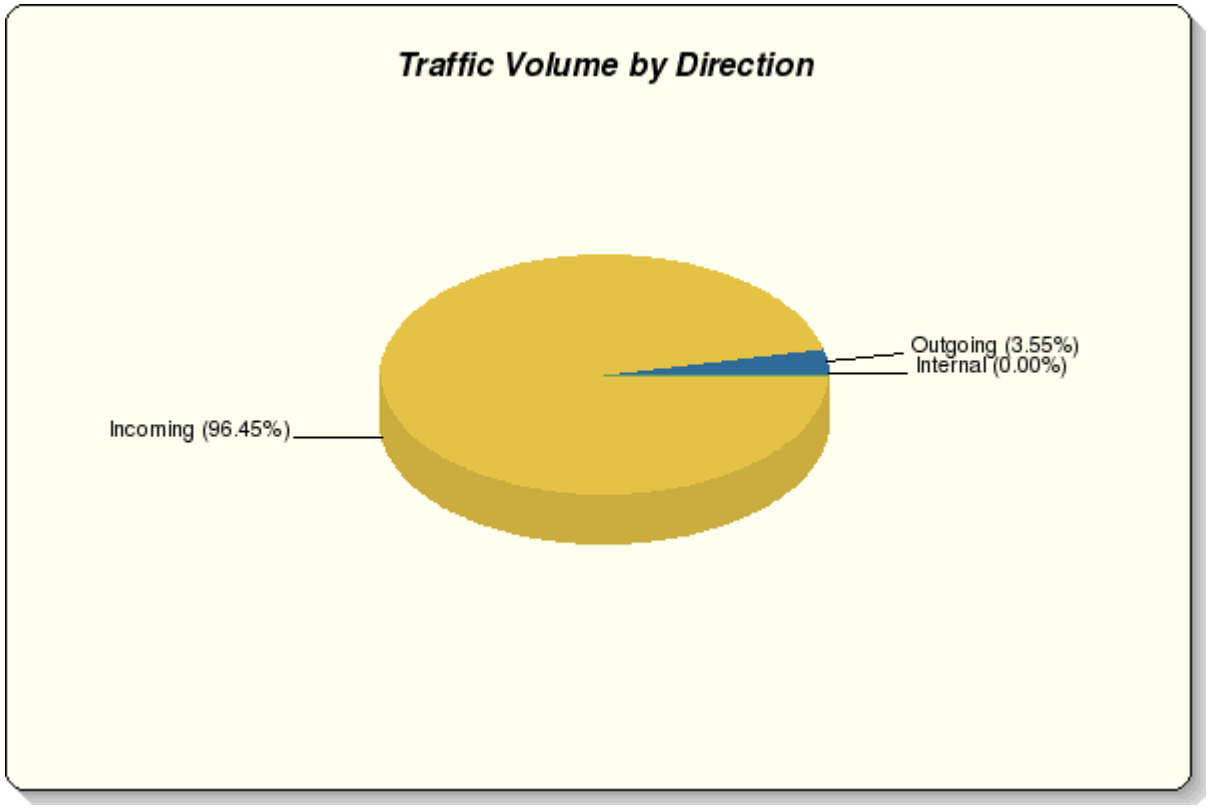
Table of Contents

Traffic Volume by Direction

The traffic volume for the reporting period, broken down by direction.

All FortiGates

Traffic Volume by Direction		
Traffic Direction	index_traffic	% of Total
Incoming	11945716541	96.45
Outgoing	439935830	3.55
Internal	288919	0.00
Total	**12385941290**	**100.00**



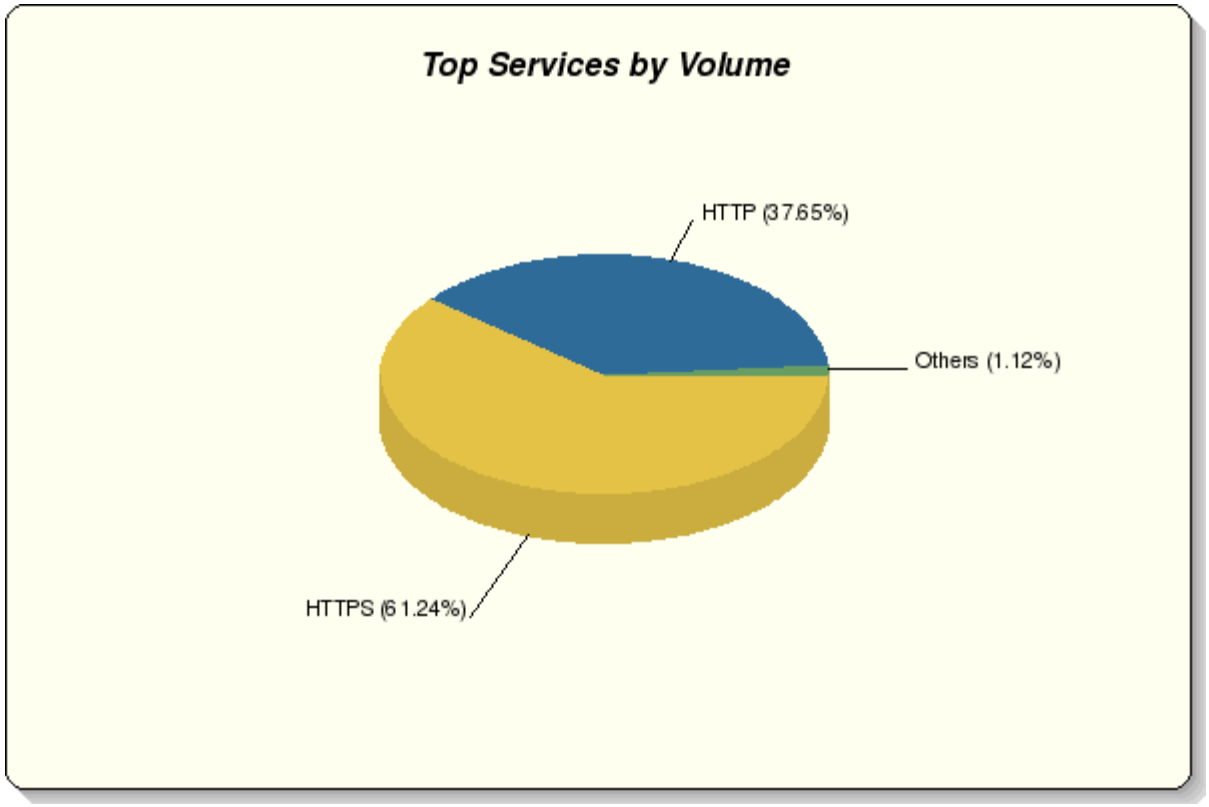
Top Services by Volume

The Internet services with the most traffic volume over the reporting period.

All FortiGates

Top Services by Volume		
Service	index_traffic	% of Total
HTTPS	7584914038	61.24
HTTP	4662791050	37.65
POP3	57427201	0.46
8200/udp	37763183	0.30
1935/tcp	14756522	0.12
1025/tcp	7826515	0.06
DNS	4428184	0.04
POP3S	3363050	0.03
IMAPS	2665594	0.02

33033/tcp	1088161	0.01
Others	8917792	0.07
Total	**12385941290**	**100.00**

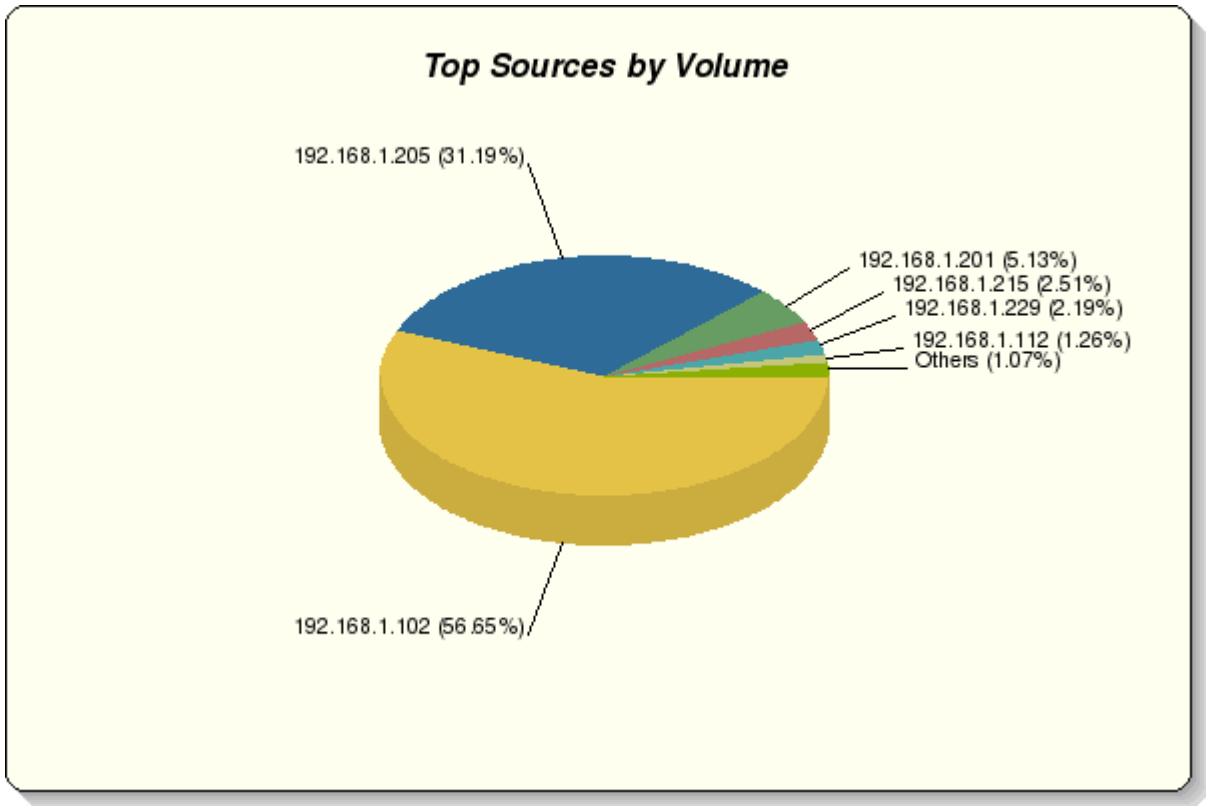


Top Sources by Volume

The sources with the most traffic volume over the reporting period.

All FortiGates

Top Sources by Volume		
User/Source	index_traffic	% of Total
192.168.1.102	7017250790	56.65
192.168.1.205	3863052889	31.19
192.168.1.201	635068070	5.13
192.168.1.215	311022593	2.51
192.168.1.229	270931784	2.19
192.168.1.112	155691810	1.26
192.168.1.203	72019051	0.58
192.168.1.211	50578062	0.41
192.168.1.202	8333685	0.07
192.168.1.204	527101	0.00
Others	1465455	0.01
Total	**12385941290**	**100.00**

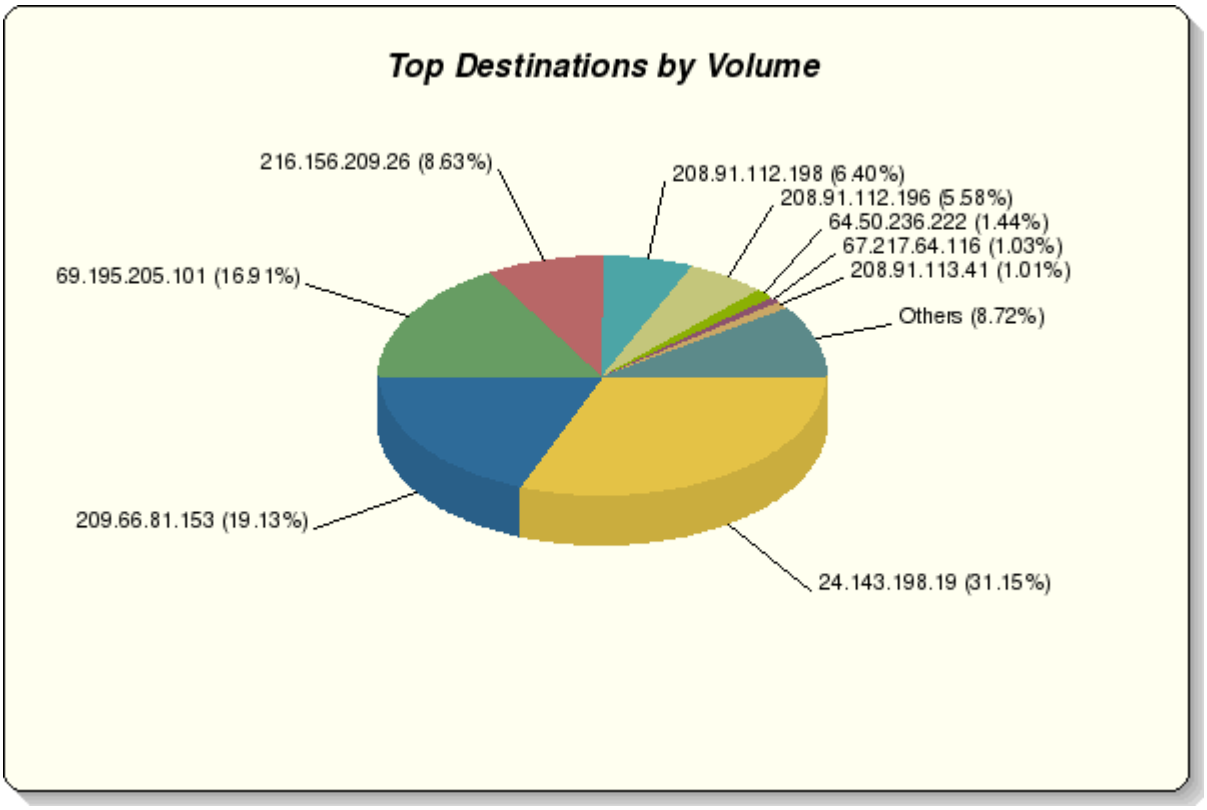


Top Destinations by Volume

The destinations with the most traffic volume over the reporting period.

All FortiGates

Top Destinations by Volume		
Destination	index_traffic	% of Total
24.143.198.19	3858083961	31.15
209.66.81.153	2368931853	19.13
69.195.205.101	2093930203	16.91
216.156.209.26	1069055144	8.63
208.91.112.198	792131041	6.40
208.91.112.196	691547971	5.58
64.50.236.222	178648983	1.44
67.217.64.116	128091777	1.03
208.91.113.41	125421128	1.01
216.155.133.132	85230893	0.69
Others	994868336	8.03
Total	**12385941290**	**100.00**



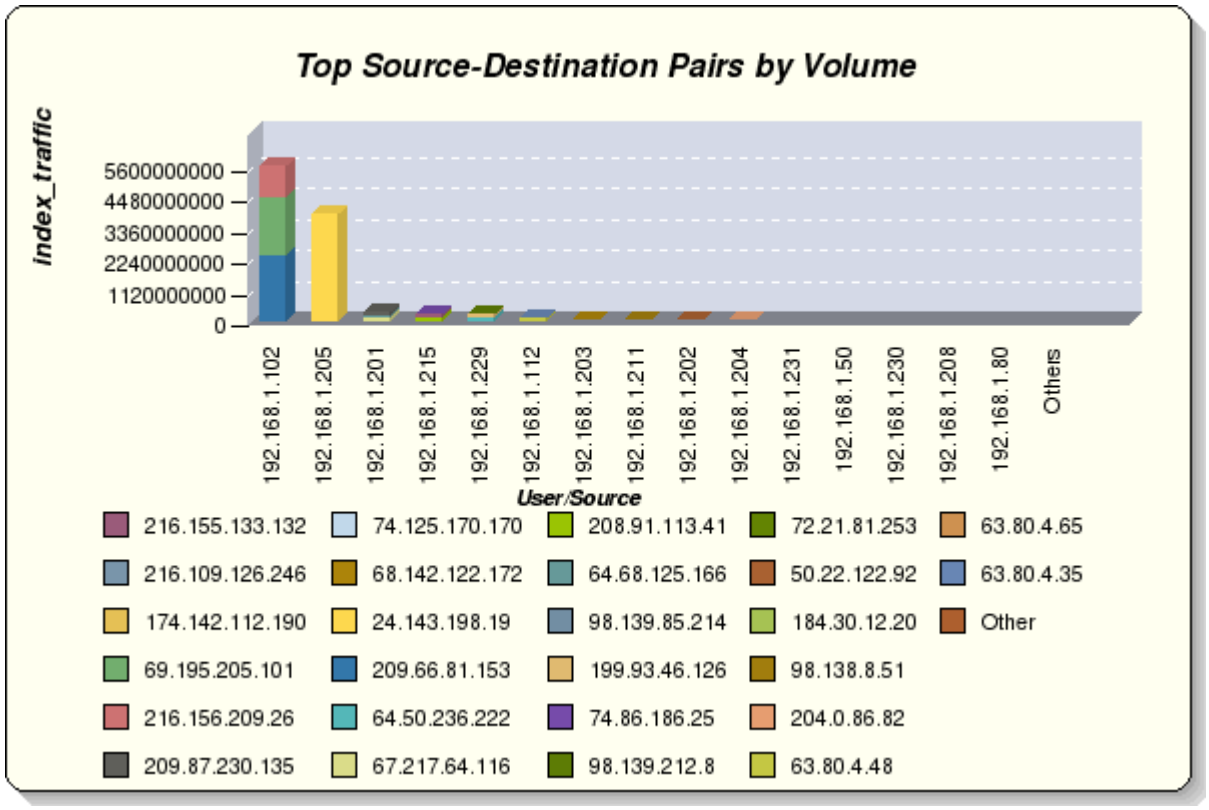
Top Source-Destination Pairs by Volume

The sources with the most traffic volume over the reporting period, broken down by destination.

All FortiGates

Top Source-Destination Pairs by Volume			
User/Source	Destination	index_traffic	% of Subtotal
192.168.1.102	209.66.81.153	2368931853	33.76
	69.195.205.101	2093930203	29.84
	216.156.209.26	1069055144	15.23
	Others	1485333590	21.17
	Subtotal	7017250790	56.65
192.168.1.205	24.143.198.19	3858083961	99.87
	63.235.20.202	414223	0.01
	74.125.227.1	318497	0.01
	Others	4236208	0.11
	Subtotal	3863052889	31.19
192.168.1.201	67.217.64.116	128091777	20.17
	64.68.125.166	75940164	11.96
	209.87.230.135	70697690	11.13
	Others	360338439	56.74
	Subtotal	635068070	5.13
192.168.1.215	208.91.113.41	125421128	40.33
	216.155.133.132	85230893	27.40
	74.86.186.25	24538431	7.89
	Others	75832141	24.38
	Subtotal	311022593	2.51
192.168.1.229	64.50.236.222	178648983	65.94

	199.93.46.126	81559193	30.10
	98.139.212.8	2342445	0.86
	Others	8381163	3.09
	Subtotal	270931784	2.19
192.168.1.112	63.80.4.48	43395450	27.87
	63.80.4.65	22406568	14.39
	63.80.4.35	20549451	13.20
	Others	69340341	44.54
	Subtotal	155691810	1.26
192.168.1.203	74.125.170.170	14118502	19.60
	174.142.112.190	10765460	14.95
	68.142.122.172	10180464	14.14
	Others	36954625	51.31
	Subtotal	72019051	0.58
192.168.1.211	98.139.85.214	15710634	31.06
	216.109.126.246	13653855	27.00
	98.138.8.51	13597273	26.88
	Others	7616300	15.06
	Subtotal	50578062	0.41
192.168.1.202	184.30.12.20	698268	8.38
	72.21.81.253	547583	6.57
	50.22.122.92	544513	6.53
	Others	6543321	78.52
	Subtotal	8333685	0.07
192.168.1.204	204.0.86.82	467459	88.68
	4.2.2.1	38431	7.29
	184.86.157.15	13502	2.56
	Others	7709	1.46
	Subtotal	527101	0.00
192.168.1.231	15.240.234.250	272436	66.36
	15.201.142.250	137155	33.41
	192.168.0.1	804	0.20
	Others	148	0.04
	Subtotal	410543	0.00
192.168.1.50	208.91.112.53	158734	40.80
	216.156.209.20	138412	35.58
	208.91.114.28	20620	5.30
	Others	71286	18.32
	Subtotal	389052	0.00
192.168.1.230	15.240.233.250	167901	100.00
	Subtotal	167901	0.00
192.168.1.208	17.155.160.27	124905	96.70
	4.2.2.1	4262	3.30
	Subtotal	129167	0.00
192.168.1.80	208.91.112.53	76721	61.43
	208.91.112.66	21117	16.91
	216.156.209.20	20006	16.02
	Others	7039	5.64
	Subtotal	124883	0.00
Others		243909	0.00
Total		**12385941290**	**100.00**



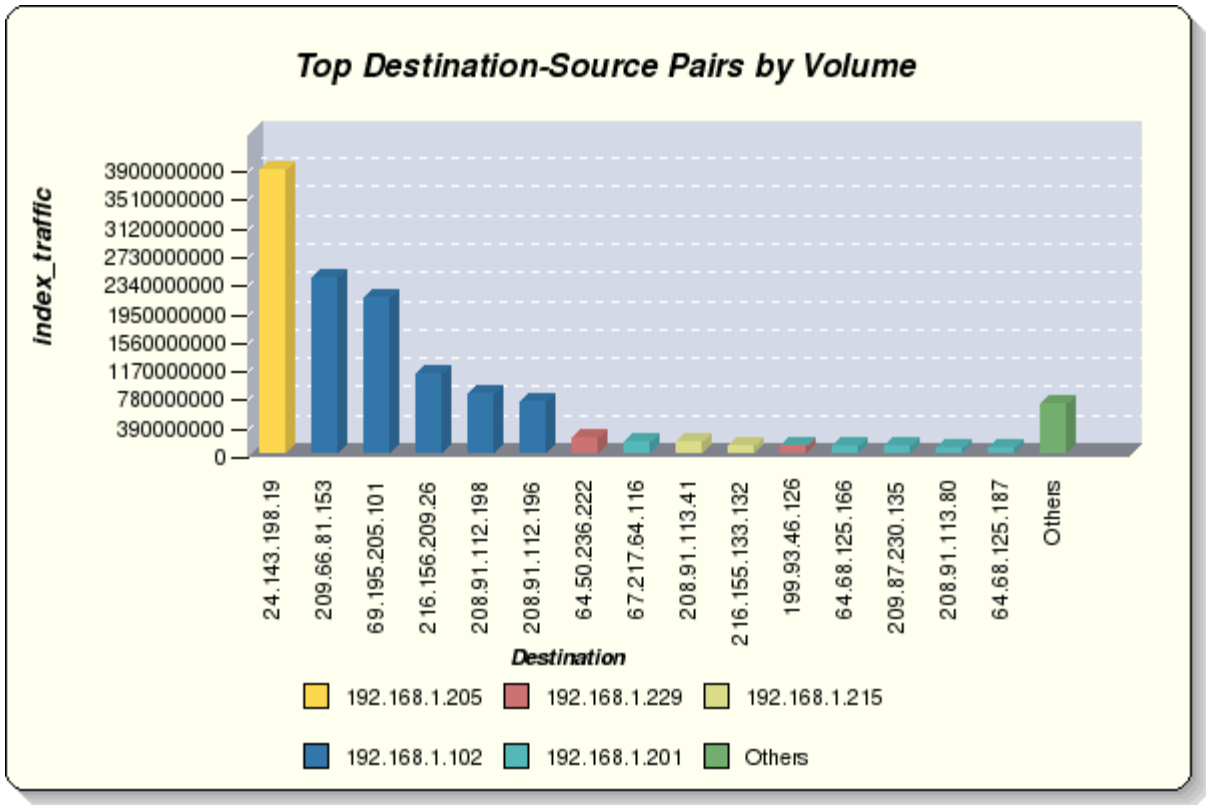
Top Destination-Source Pairs by Volume

The destinations with the most traffic volume over the reporting period, broken down by source.

All FortiGates

Top Destination-Source Pairs by Volume			
Destination	User/Source	index_traffic	% of Subtotal
24.143.198.19	192.168.1.205	3858083961	100.00
	Subtotal	3858083961	31.15
209.66.81.153	192.168.1.102	2368931853	100.00
	Subtotal	2368931853	19.13
69.195.205.101	192.168.1.102	2093930203	100.00
	Subtotal	2093930203	16.91
216.156.209.26	192.168.1.102	1069055144	100.00
	Subtotal	1069055144	8.63
208.91.112.198	192.168.1.102	792131041	100.00
	Subtotal	792131041	6.40
208.91.112.196	192.168.1.102	691547971	100.00
	Subtotal	691547971	5.58
64.50.236.222	192.168.1.229	178648983	100.00
	Subtotal	178648983	1.44
67.217.64.116	192.168.1.201	128091777	100.00
	Subtotal	128091777	1.03
208.91.113.41	192.168.1.215	125421128	100.00
	Subtotal	125421128	1.01
216.155.133.132	192.168.1.215	85230893	100.00
	Subtotal	85230893	0.69
199.93.46.126	192.168.1.229	81559193	99.93

	192.168.1.201	53417	0.07
	Subtotal	81612610	0.66
64.68.125.166	192.168.1.201	75940164	100.00
	Subtotal	75940164	0.61
209.87.230.135	192.168.1.201	70697690	100.00
	Subtotal	70697690	0.57
208.91.113.80	192.168.1.201	63655442	100.00
	Subtotal	63655442	0.51
64.68.125.187	192.168.1.201	48325460	100.00
	Subtotal	48325460	0.39
Others		654636970	5.29
Total		**12385941290**	**100.00**



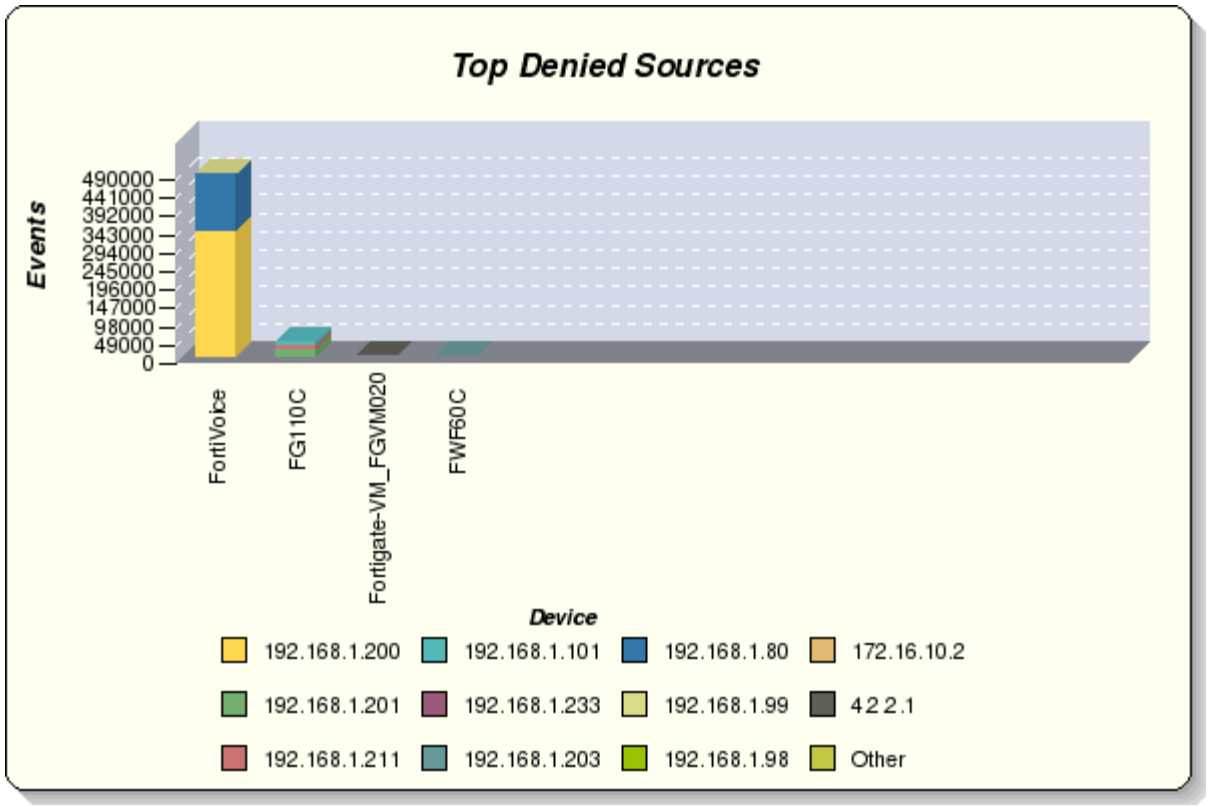
Top Denied Sources

The sources with the most policy violation attempts.

All FortiGates

Top Denied Sources			
Device	User/Source	Events	% of Subtotal
FortiVoice	192.168.1.200	333411	68.86
	192.168.1.80	147946	30.55
	192.168.1.99	2290	0.47
	Others	568	0.12
	Subtotal	484215	87.65
FG110C	192.168.1.201	19091	29.61
	192.168.1.211	12110	18.79
	192.168.1.101	7277	11.29
	Others	25988	40.31

	Subtotal	64466	11.67
Fortigate-VM_FGVM020000001140	192.168.1.98	921	39.75
	192.168.1.233	516	22.27
	4.2.2.1	76	3.28
	Others	804	34.70
	Subtotal	2317	0.42
FWF60C	192.168.1.201	591	41.80
	172.16.10.2	331	23.41
	192.168.1.203	148	10.47
	Others	344	24.33
	Subtotal	1414	0.26
Total		**552412**	**100.00**



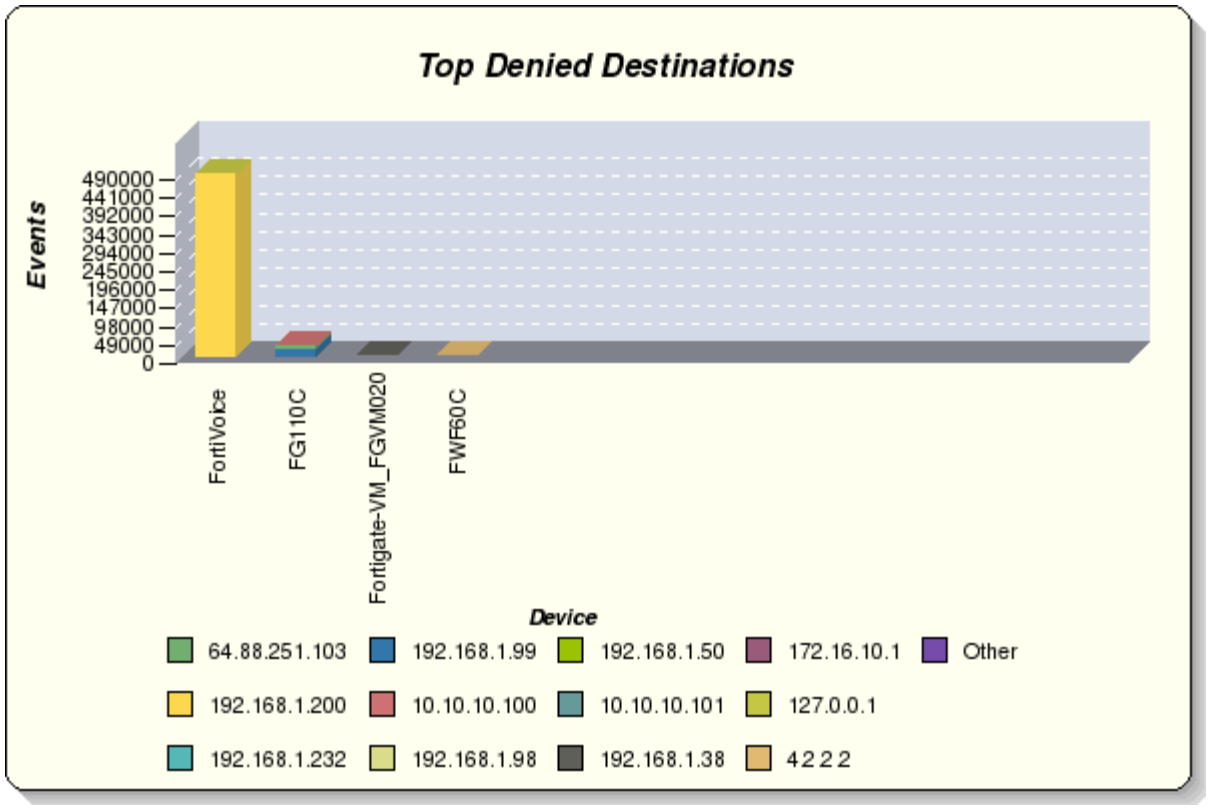
Top Denied Destinations

The destination with the most policy violation attempts.

All FortiGates

Top Denied Destinations			
Device	Destination	Events	% of Subtotal
FortiVoice	192.168.1.200	484205	100.00
	10.10.10.101	7	0.00
	127.0.0.1	3	0.00
	Subtotal	484215	87.65
FG110C	192.168.1.99	20198	31.33
	64.88.251.103	3627	5.63
	10.10.10.100	2082	3.23
	Others	38559	59.81
	Subtotal	64466	11.67

Fortigate-VM_FGVM020000001140	192.168.1.232	1343	57.96
	192.168.1.98	966	41.69
	192.168.1.38	4	0.17
	Others	4	0.17
	Subtotal	2317	0.42
FWF60C	192.168.1.50	563	39.82
	172.16.10.1	170	12.02
	4.2.2.2	96	6.79
	Others	585	41.37
	Subtotal	1414	0.26
Total		**552412**	**100.00**



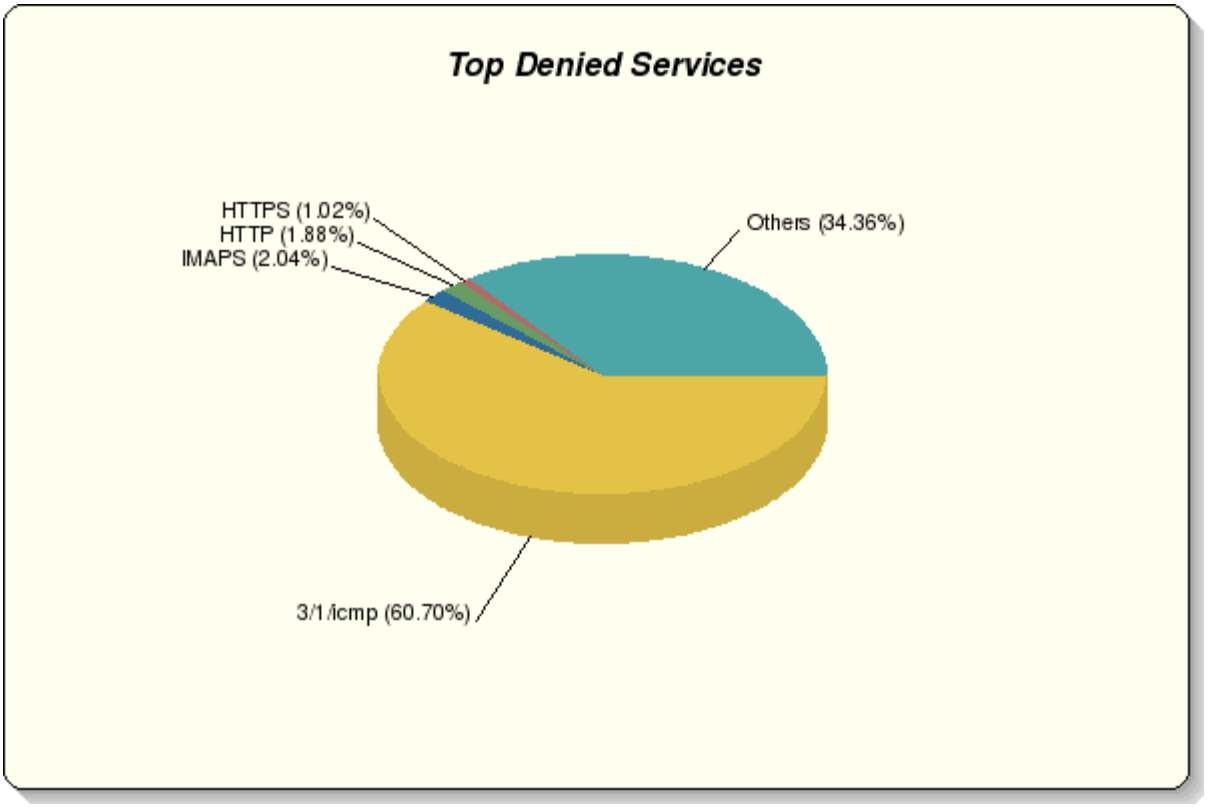
Top Denied Services

The Internet services with the most policy violation attempts.

All FortiGates

Top Denied Services		
Service	Events	% of Total
3/1/icmp	335341	60.70
IMAPS	11256	2.04
HTTP	10360	1.88
HTTPS	5649	1.02
5/1/icmp	4974	0.90
5223/tcp	3993	0.72
X-WINDOWS	3672	0.66
NTP	3401	0.62
DNS	2741	0.50
MMS	2241	0.41

Others	168784	30.55
Total	**552412**	**100.00**

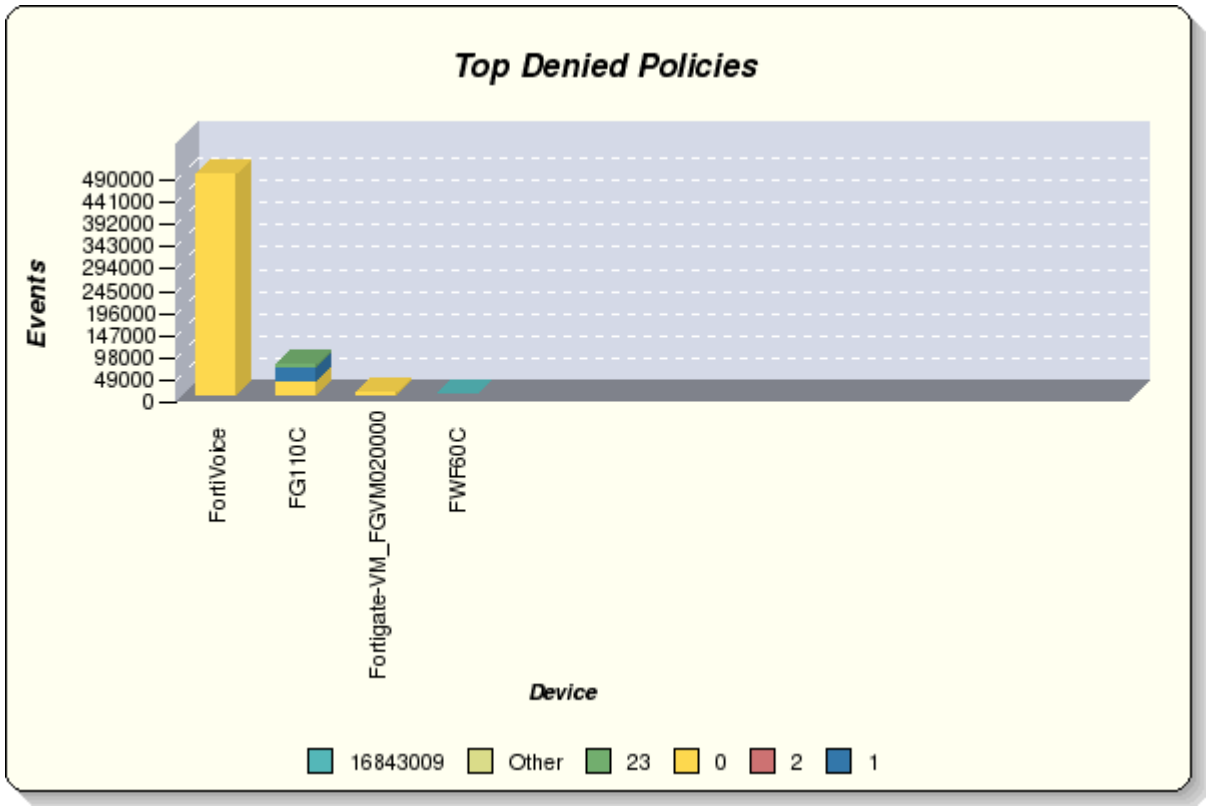


Top Denied Policies

The firewall policies with the most violation attempts.

All FortiGates

Top Denied Policies			
Device	Policy ID	Events	% of Subtotal
FortiVoice	0	484215	100.00
	Subtotal	484215	87.65
FG110C	1	30114	46.71
	0	29327	45.49
	23	4813	7.47
	Others	212	0.33
	Subtotal	64466	11.67
Fortigate-VM_FGVM020000001140	0	2317	100.00
	Subtotal	2317	0.42
FWF60C	0	1411	99.79
	2	2	0.14
	16843009	1	0.07
	Subtotal	1414	0.26
Total		**552412**	**100.00**

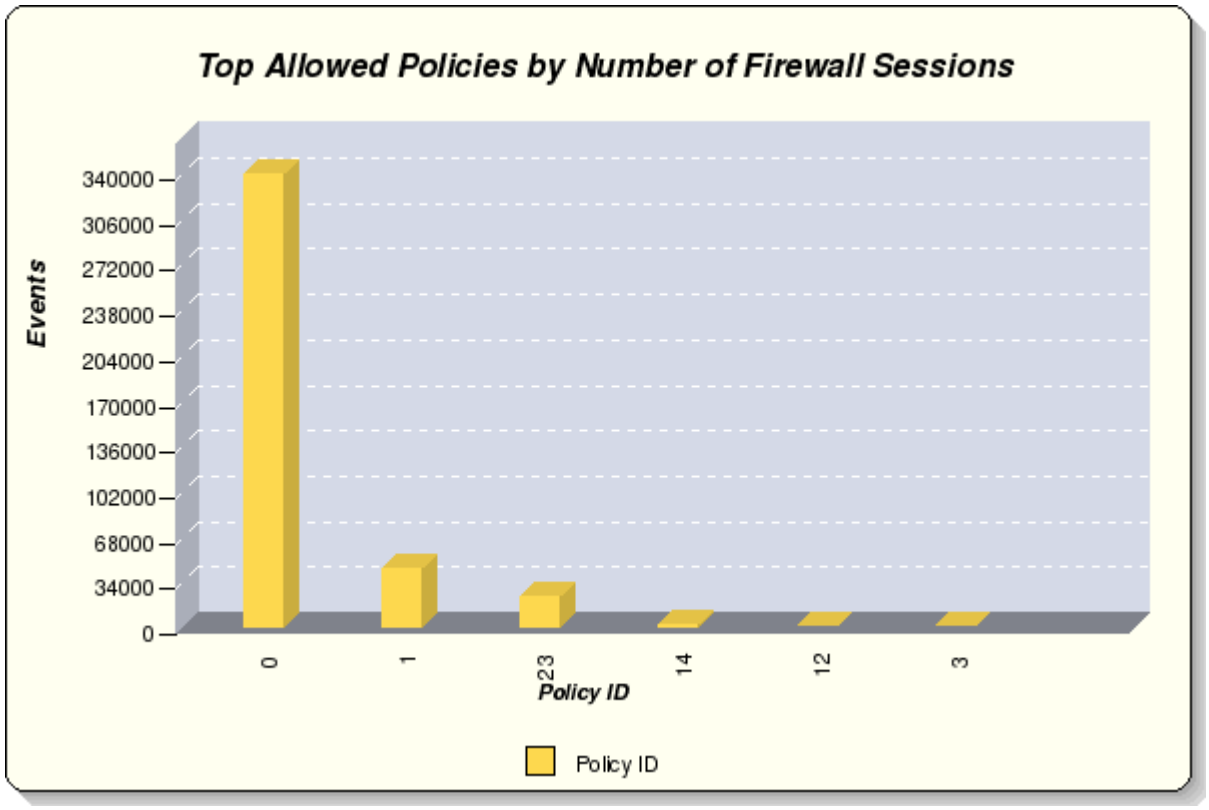


Top Allowed Policies by Number of Firewall Sessions

The firewall policies with the most allowed sessions.

All FortiGates

Top Allowed Policies by Number of Firewall Sessions		
Policy ID	Events	% of Total
0	337925	83.17
1	43595	10.73
23	22152	5.45
14	2203	0.54
12	232	0.06
3	180	0.04
Total	**406287**	**100.00**

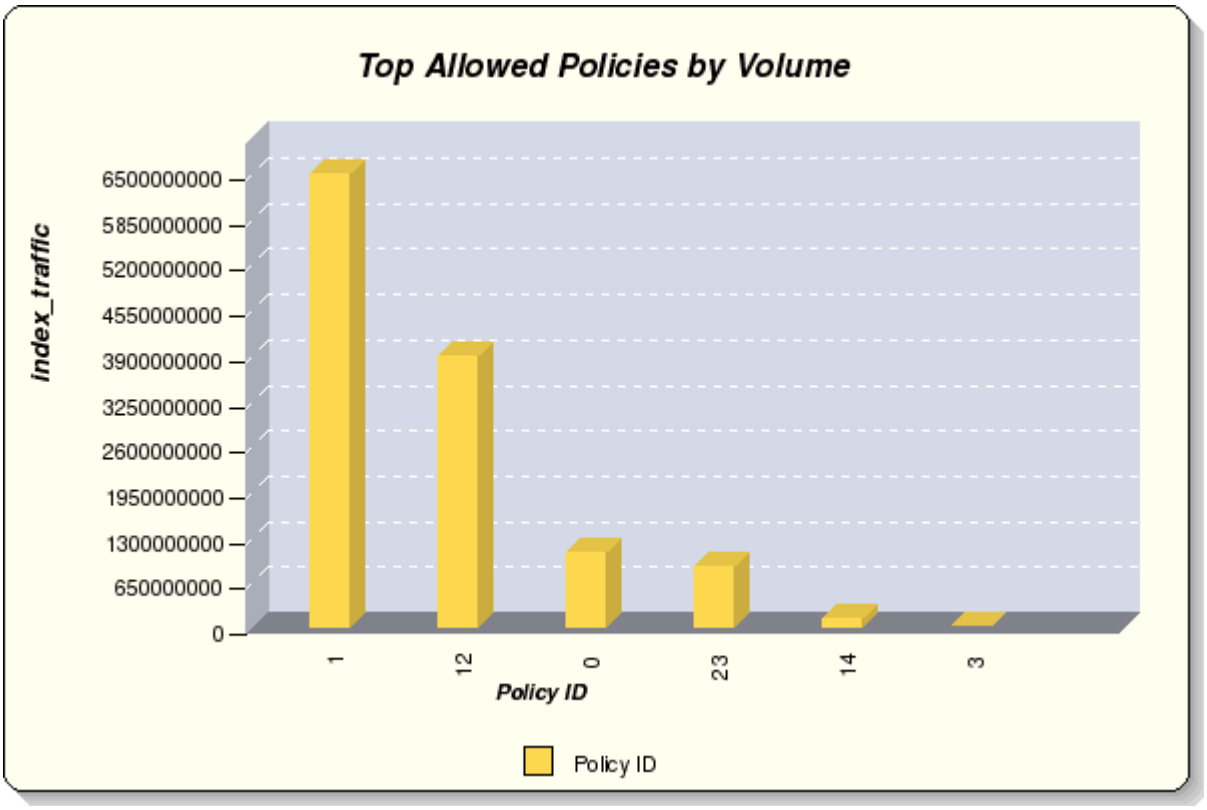


Top Allowed Policies by Volume

The firewall policies with the most allowed traffic volume.

All FortiGates

Top Allowed Policies by Volume		
Policy ID	index_traffic	% of Total
1	6475135639	52.28
12	3861215978	31.17
0	1068646068	8.63
23	850915765	6.87
14	128653898	1.04
3	1373942	0.01
Total	**12385941290**	**100.00**

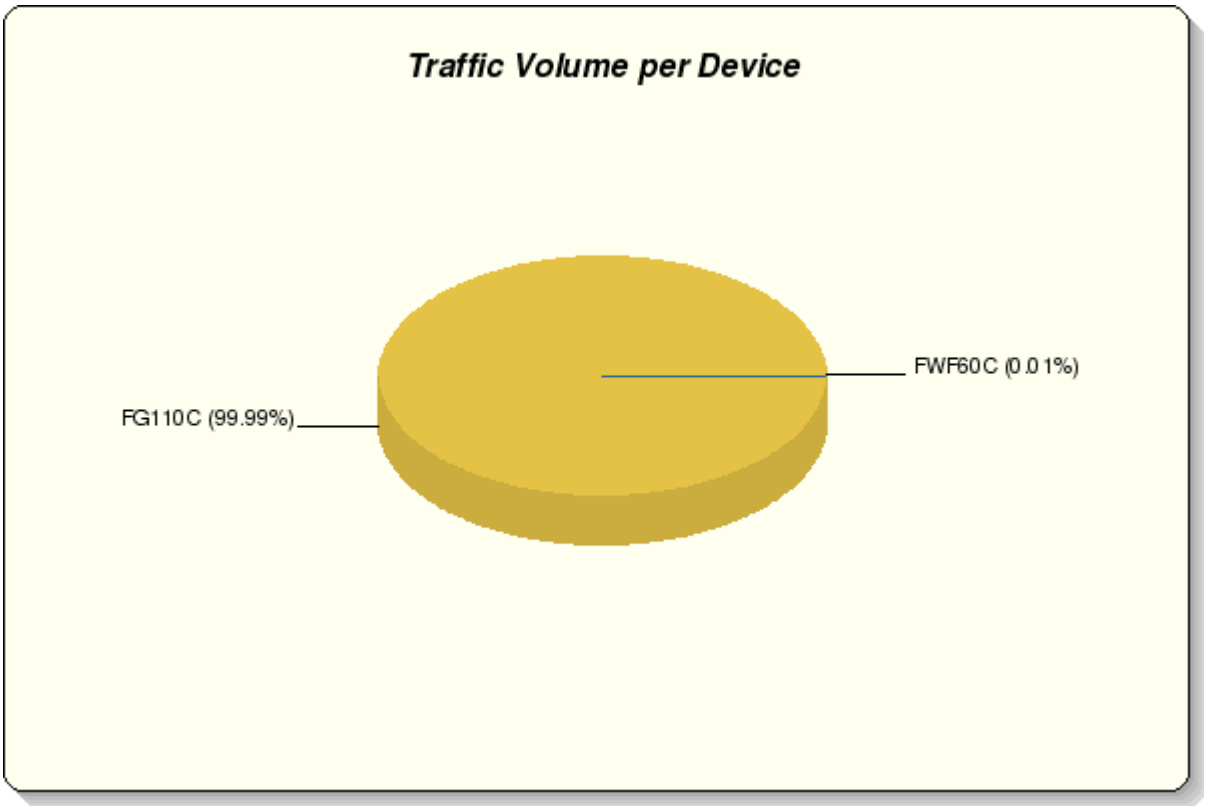


Traffic Volume per Device

The traffic volume over the reporting period, broken down by device.

All FortiGates

Traffic Volume per Device		
Device	index_traffic	% of Total
FG110C	12384567348	99.99
FWF60C	1373942	0.01
Total	**12385941290**	**100.00**



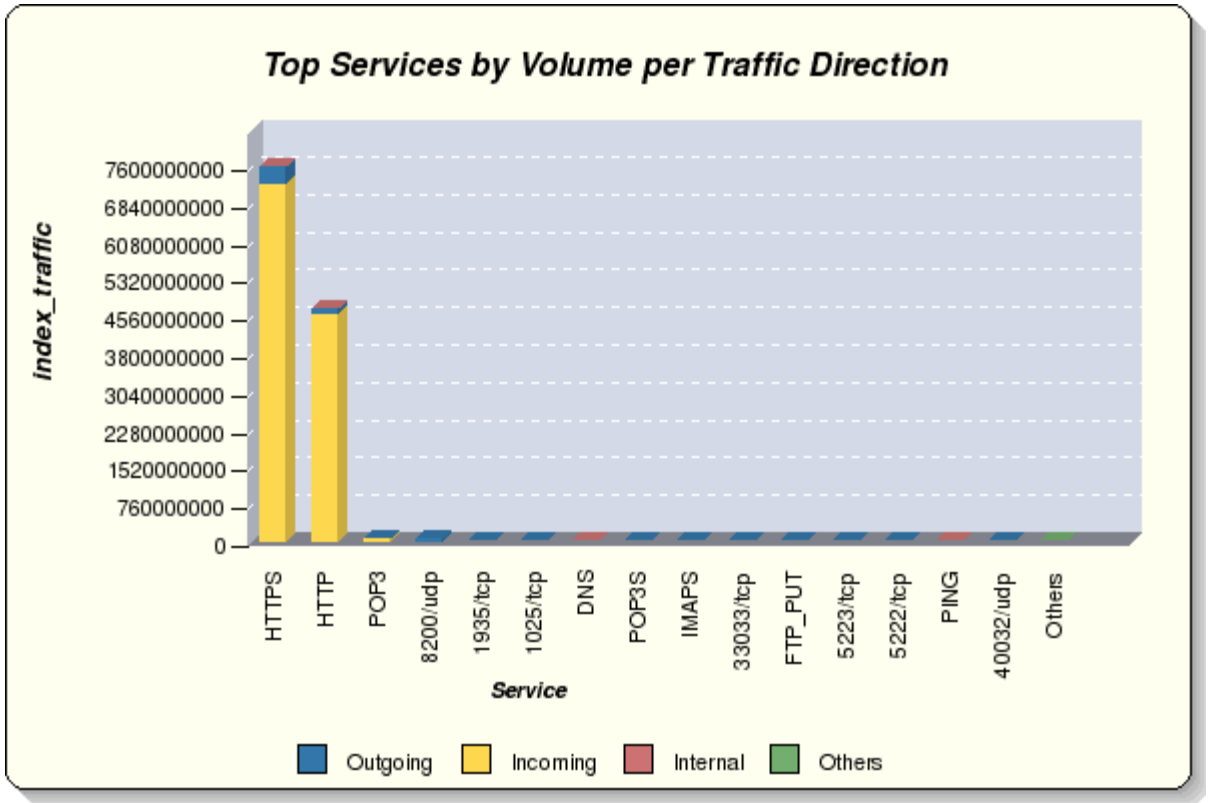
Top Services by Volume per Traffic Direction

The Internet services with the most traffic volume over the reporting period, broken down by direction.

All FortiGates

Top Services by Volume per Traffic Direction			
Service	Traffic Direction	index_traffic	% of Subtotal
HTTPS	Incoming	7253611953	95.63
	Outgoing	331300717	4.37
	Internal	1368	0.00
	Subtotal	7584914038	61.24
HTTP	Incoming	4595215954	98.55
	Outgoing	67573968	1.45
	Internal	1128	0.00
	Subtotal	4662791050	37.65
POP3	Incoming	56059474	97.62
	Outgoing	1367727	2.38
	Subtotal	57427201	0.46
8200/udp	Outgoing	24612154	65.17
	Incoming	13151029	34.83
	Subtotal	37763183	0.30
1935/tcp	Incoming	14533027	98.49
	Outgoing	223495	1.51
	Subtotal	14756522	0.12
1025/tcp	Outgoing	7398920	94.54
	Incoming	427595	5.46
	Subtotal	7826515	0.06
DNS	Incoming	3056224	69.02

	Outgoing	1371156	30.96
	Internal	804	0.02
	Subtotal	4428184	0.04
POP3S	Incoming	2950577	87.74
	Outgoing	412473	12.26
	Subtotal	3363050	0.03
IMAPS	Incoming	2350948	88.20
	Outgoing	314646	11.80
	Subtotal	2665594	0.02
33033/tcp	Outgoing	734053	67.46
	Incoming	354108	32.54
	Subtotal	1088161	0.01
FTP_PUT	Incoming	546760	95.75
	Outgoing	24252	4.25
	Subtotal	571012	0.00
5223/tcp	Incoming	275025	52.65
	Outgoing	247337	47.35
	Subtotal	522362	0.00
5222/tcp	Outgoing	240162	58.63
	Incoming	169429	41.37
	Subtotal	409591	0.00
PING	Internal	253932	100.00
	Subtotal	253932	0.00
40032/udp	Incoming	96492	79.91
	Outgoing	24252	20.09
	Subtotal	120744	0.00
Others		7040151	0.06
Total		**12385941290**	**100.00**



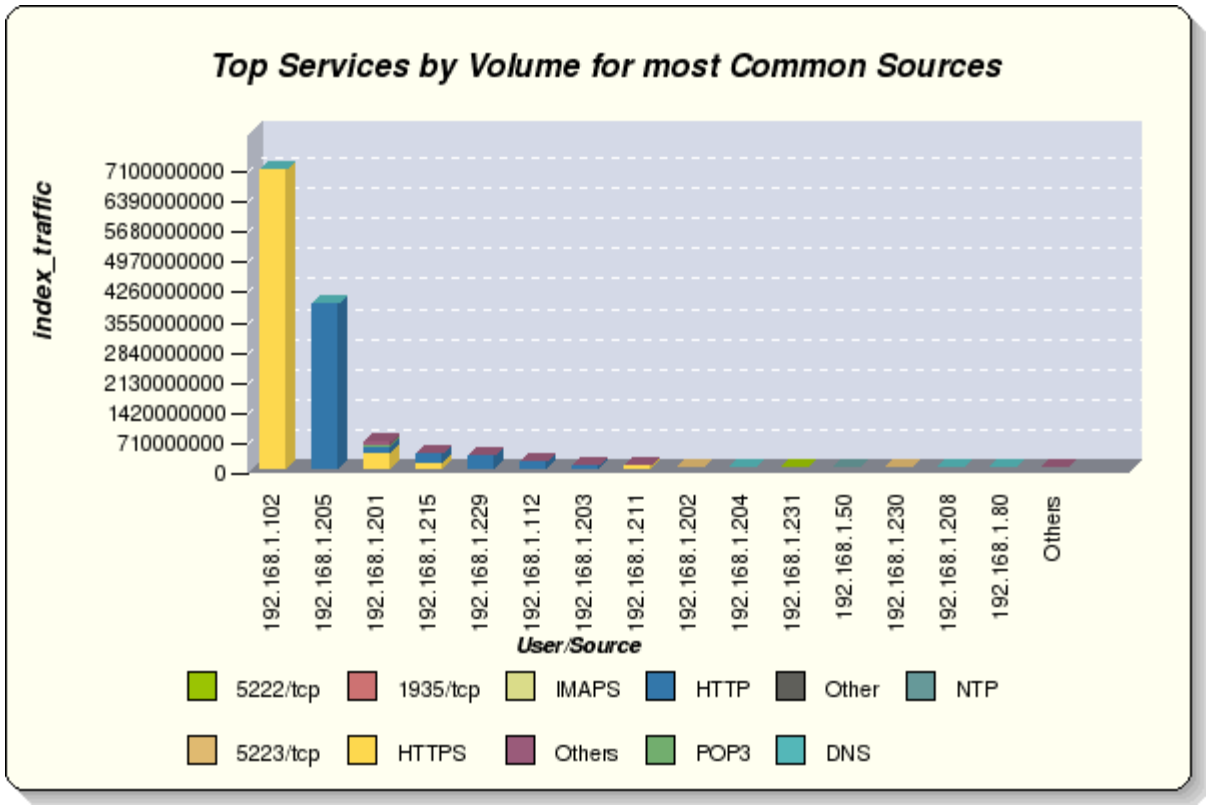
Top Services by Volume for most Common Sources

The sources with the most traffic volume over the reporting period, broken down by Internet service.

All FortiGates

Top Services by Volume for most Common Sources			
User/Source	Service	index_traffic	% of Subtotal
192.168.1.102	HTTPS	7017246308	100.00
	DNS	4482	0.00
	Subtotal	7017250790	56.65
192.168.1.205	HTTP	3862286357	99.98
	HTTPS	726641	0.02
	DNS	39891	0.00
	Subtotal	3863052889	31.19
192.168.1.201	HTTPS	380426498	59.90
	HTTP	138363322	21.79
	POP3	57427201	9.04
	Others	58851049	9.27
	Subtotal	635068070	5.13
192.168.1.215	HTTP	175884718	56.55
	HTTPS	133999519	43.08
	DNS	677628	0.22
	Others	460728	0.15
	Subtotal	311022593	2.51
192.168.1.229	HTTP	268734263	99.19
	HTTPS	1991884	0.74
	DNS	172003	0.06
	Others	33634	0.01
	Subtotal	270931784	2.19
192.168.1.112	HTTP	152724987	98.09
	HTTPS	1911900	1.23
	IMAPS	957661	0.62
	Others	97262	0.06
	Subtotal	155691810	1.26
192.168.1.203	HTTP	55285418	76.76
	1935/tcp	14679343	20.38
	HTTPS	1960517	2.72
	Others	93773	0.13
	Subtotal	72019051	0.58
192.168.1.211	HTTPS	45196489	89.36
	HTTP	2007467	3.97
	DNS	1784323	3.53
	Others	1589783	3.14
	Subtotal	50578062	0.41
192.168.1.202	HTTP	6941748	83.30
	HTTPS	1051152	12.61
	5223/tcp	165587	1.99
	Others	175198	2.10
	Subtotal	8333685	0.07
192.168.1.204	HTTP	488670	92.71
	DNS	38431	7.29
	Subtotal	527101	0.00
192.168.1.231	5222/tcp	409591	99.77
	DNS	952	0.23
	Subtotal	410543	0.00
192.168.1.50	HTTPS	180478	46.39
	DNS	159986	41.12

	NTP	27968	7.19
	Others	20620	5.30
	Subtotal	389052	0.00
192.168.1.230	5223/tcp	167901	100.00
	Subtotal	167901	0.00
192.168.1.208	HTTPS	124905	96.70
	DNS	4262	3.30
	Subtotal	129167	0.00
192.168.1.80	DNS	76721	61.43
	HTTPS	48162	38.57
	Subtotal	124883	0.00
Others		243909	0.00
Total		**12385941290**	**100.00**



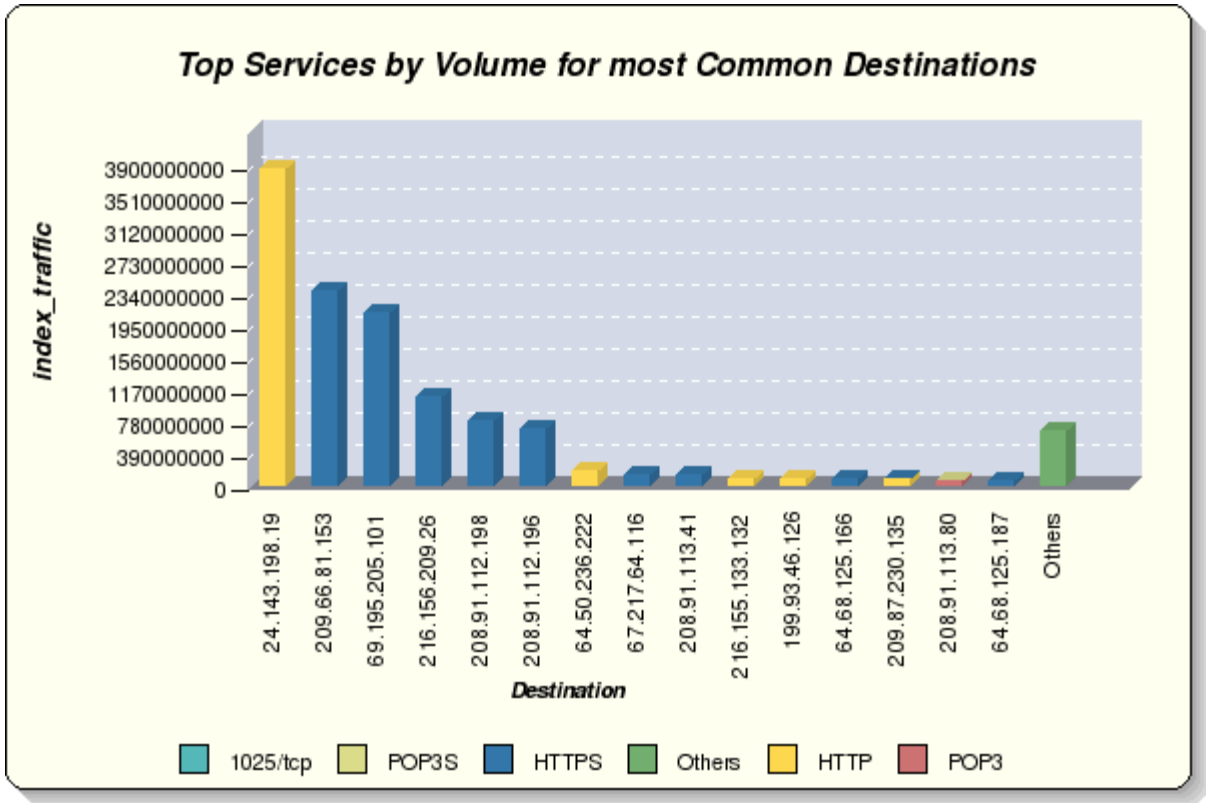
Top Services by Volume for most Common Destinations

The destinations with the most traffic volume over the reporting period, broken down by Internet service.

All FortiGates

Top Services by Volume for most Common Destinations			
Destination	Service	index_traffic	% of Subtotal
24.143.198.19	HTTP	3858083961	100.00
	Subtotal	3858083961	31.15
209.66.81.153	HTTPS	2368931853	100.00
	Subtotal	2368931853	19.13
69.195.205.101	HTTPS	2093930203	100.00
	Subtotal	2093930203	16.91
216.156.209.26	HTTPS	1069055144	100.00

	Subtotal	1069055144	8.63
208.91.112.198	HTTPS	792131041	100.00
	Subtotal	792131041	6.40
208.91.112.196	HTTPS	691547971	100.00
	Subtotal	691547971	5.58
64.50.236.222	HTTP	178648983	100.00
	Subtotal	178648983	1.44
67.217.64.116	HTTPS	128091777	100.00
	Subtotal	128091777	1.03
208.91.113.41	HTTPS	125421128	100.00
	Subtotal	125421128	1.01
216.155.133.132	HTTP	85230893	100.00
	Subtotal	85230893	0.69
199.93.46.126	HTTP	81612610	100.00
	Subtotal	81612610	0.66
64.68.125.166	HTTPS	75940164	100.00
	Subtotal	75940164	0.61
209.87.230.135	HTTP	70521043	99.75
	HTTPS	176647	0.25
	Subtotal	70697690	0.57
208.91.113.80	POP3	55796639	87.65
	1025/tcp	7826515	12.30
	POP3S	32288	0.05
	Subtotal	63655442	0.51
64.68.125.187	HTTPS	48325460	100.00
	Subtotal	48325460	0.39
Others		654636970	5.29
Total		**12385941290**	**100.00**

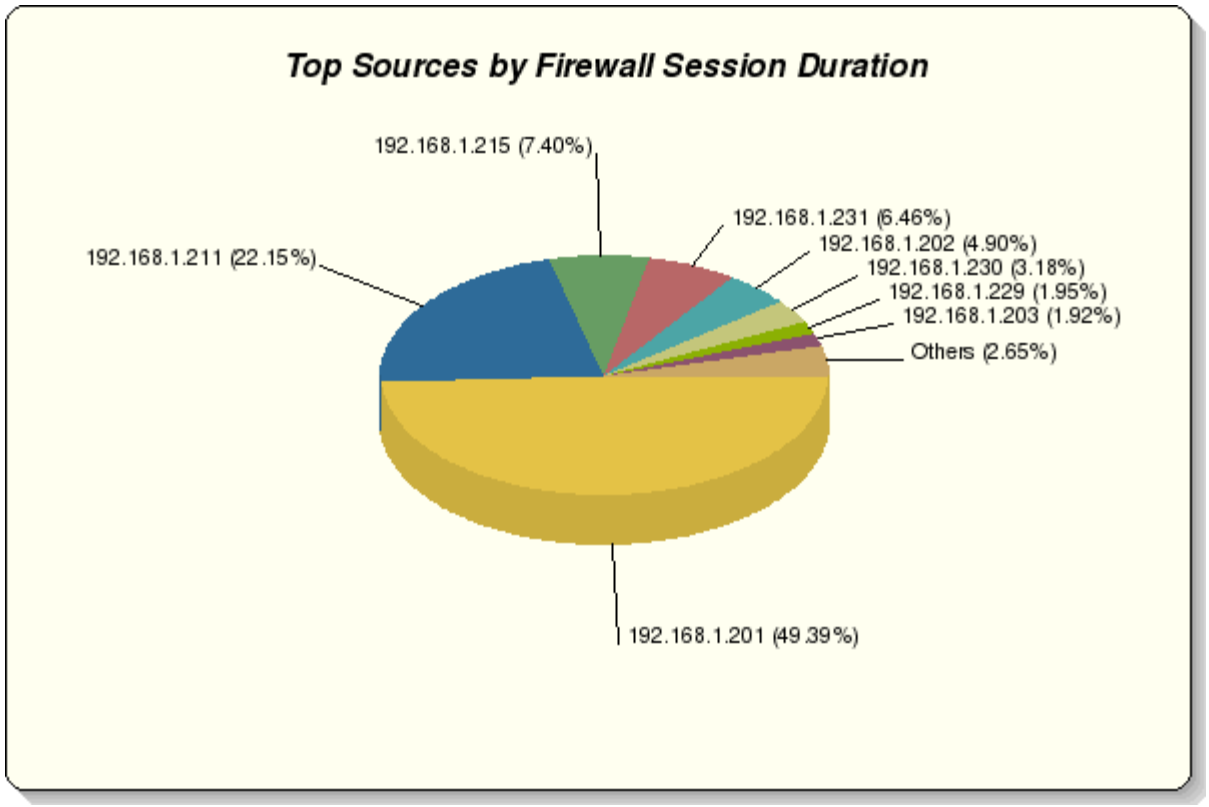


Top Sources by Firewall Session Duration

The sources with the longest cumulated traffic duration over the reporting period.

All FortiGates

Top Sources by Firewall Session Duration		
User/Source	Duration (sec)	% of Total
192.168.1.201	5757.52	49.39
192.168.1.211	2581.93	22.15
192.168.1.215	862.69	7.40
192.168.1.231	752.64	6.46
192.168.1.202	571.04	4.90
192.168.1.230	370.46	3.18
192.168.1.229	226.82	1.95
192.168.1.203	223.54	1.92
192.168.1.50	84.81	0.73
192.168.1.205	58.49	0.50
Others	166.14	1.43
Total	**11656.09**	**100.00**



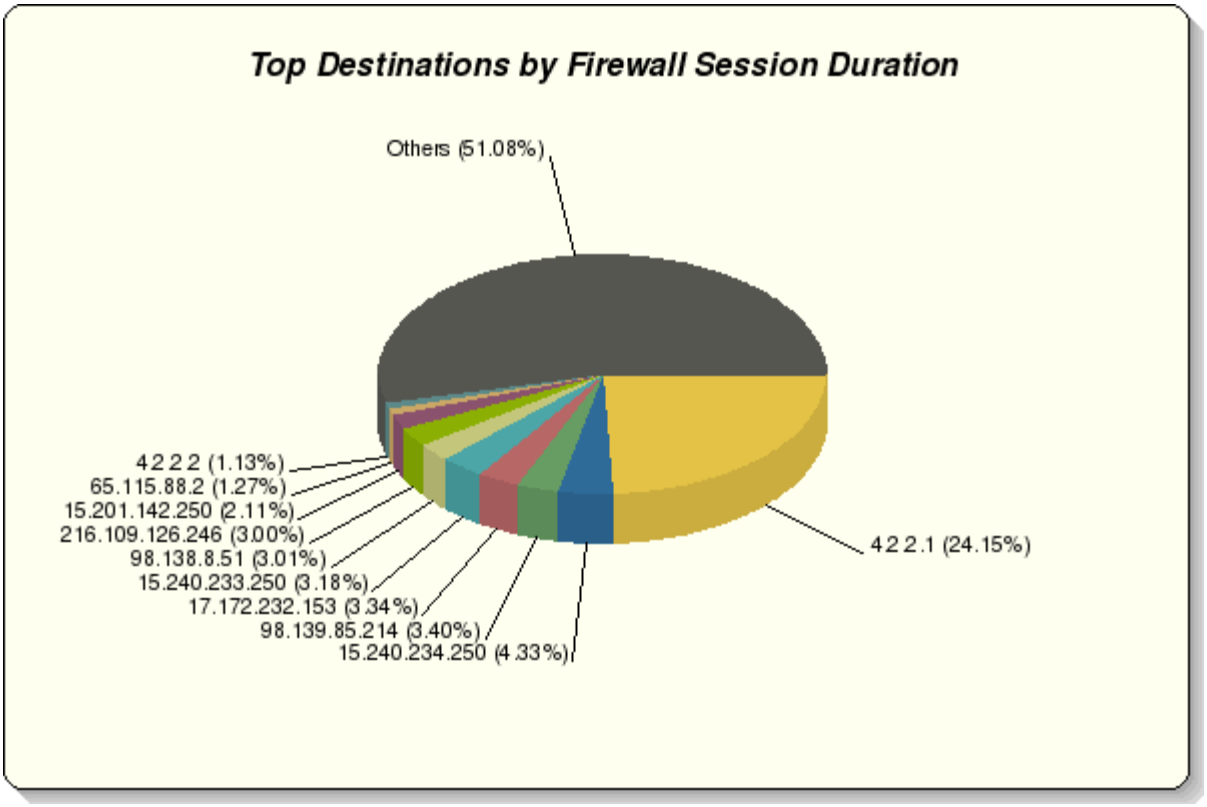
Top Destinations by Firewall Session Duration

The destinations with the longest cumulated traffic duration over the reporting period.

All FortiGates

Top Destinations by Firewall Session Duration		
Host Name	Duration (min)	% of Total
4.2.2.1	46.91	24.15
15.240.234.250	8.41	4.33
98.139.85.214	6.60	3.40

17.172.232.153	6.48	3.34
15.240.233.250	6.17	3.18
98.138.8.51	5.85	3.01
216.109.126.246	5.83	3.00
15.201.142.250	4.11	2.11
65.115.88.2	2.47	1.27
4.2.2.2	2.20	1.13
Others	99.24	51.08
Total	**194.27**	**100.00**

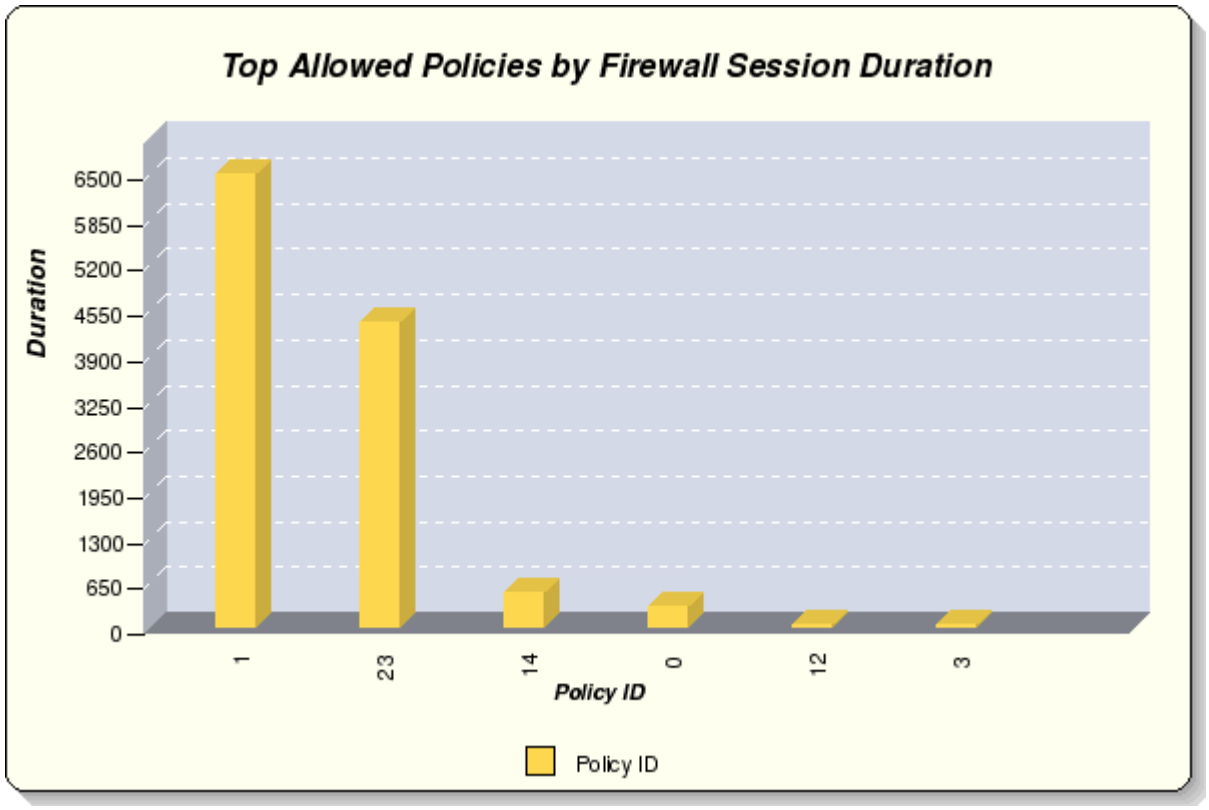


Top Allowed Policies by Firewall Session Duration

The firewall policies with the most allowed session duration.

All FortiGates

Top Allowed Policies by Firewall Session Duration		
Policy ID	Duration (sec)	% of Total
1	6482.73	55.62
23	4344.58	37.27
14	479.51	4.11
0	274.80	2.36
12	39.12	0.34
3	35.35	0.30
Total	**11656.09**	**100.00**

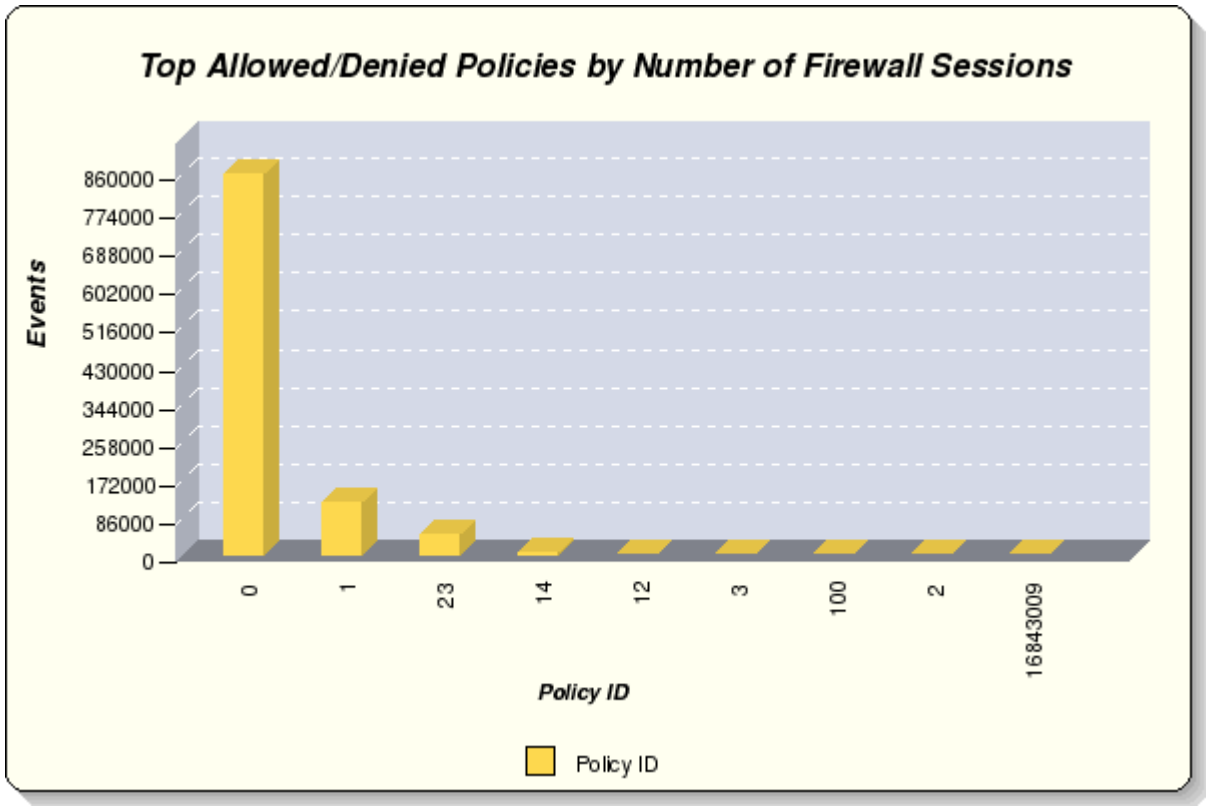


Top Allowed/Denied Policies by Number of Firewall Sessions

The firewall policies with the most allowed/denied sessions.

All FortiGates

Top Allowed/Denied Policies by Number of Firewall Sessions		
Policy ID	Events	% of Total
0	855195	83.57
1	115970	11.33
23	46676	4.56
14	4655	0.45
12	463	0.05
3	375	0.04
100	3	0.00
2	2	0.00
16843009	1	0.00
Total	**1023340**	**100.00**



Traffic_by_Devices_with_Hits

Traffic_by_Devices_with_Hits_Desc

All FortiGates

Traffic_by_Devices_with_Hits			
Device	Hits	Volume(MB)	Volume(%)
FG110C	68246	11810.84	99.99%
FWF60C	219	1.31	0.01%
Total	**406287**	**11812.15(MB)**	**100.00%**