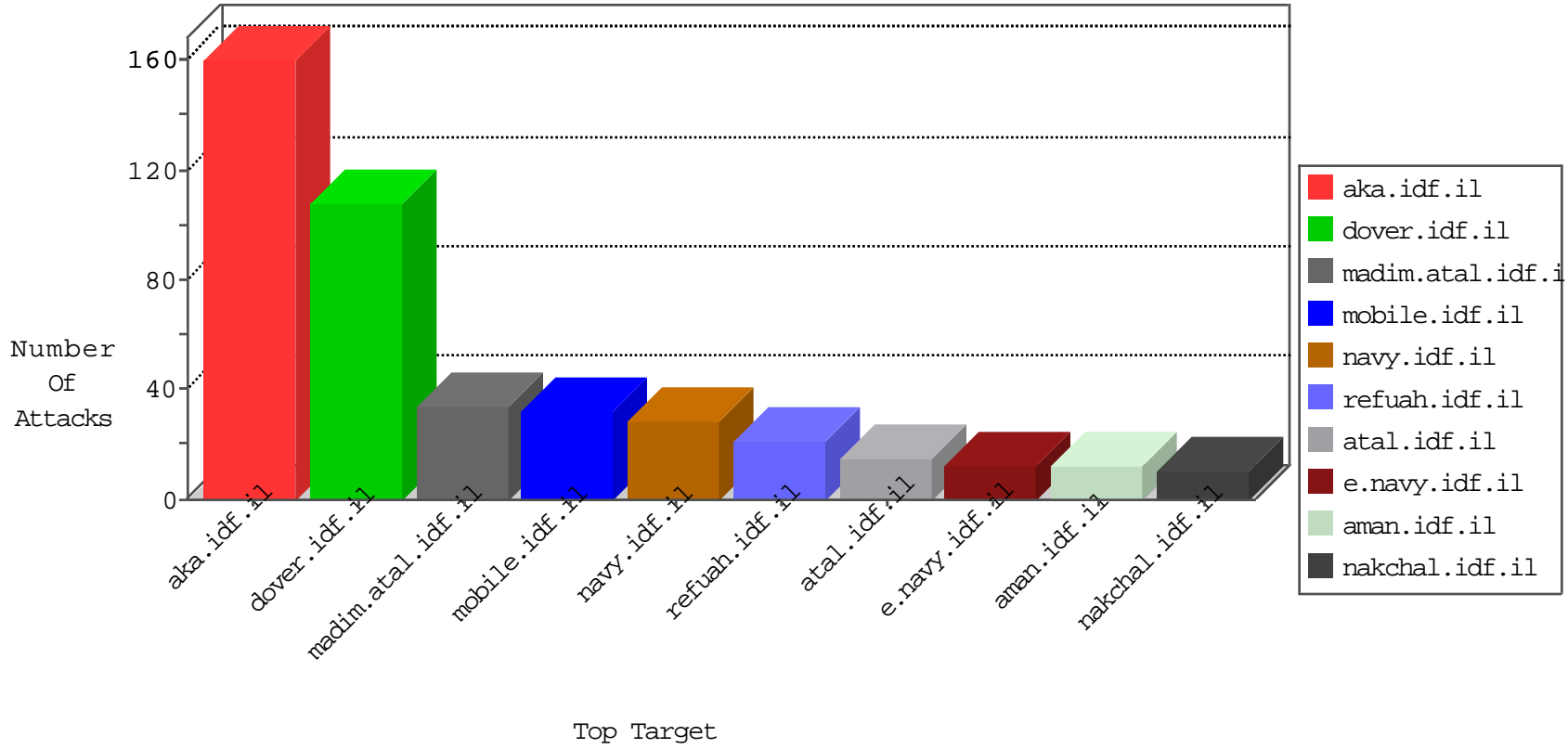


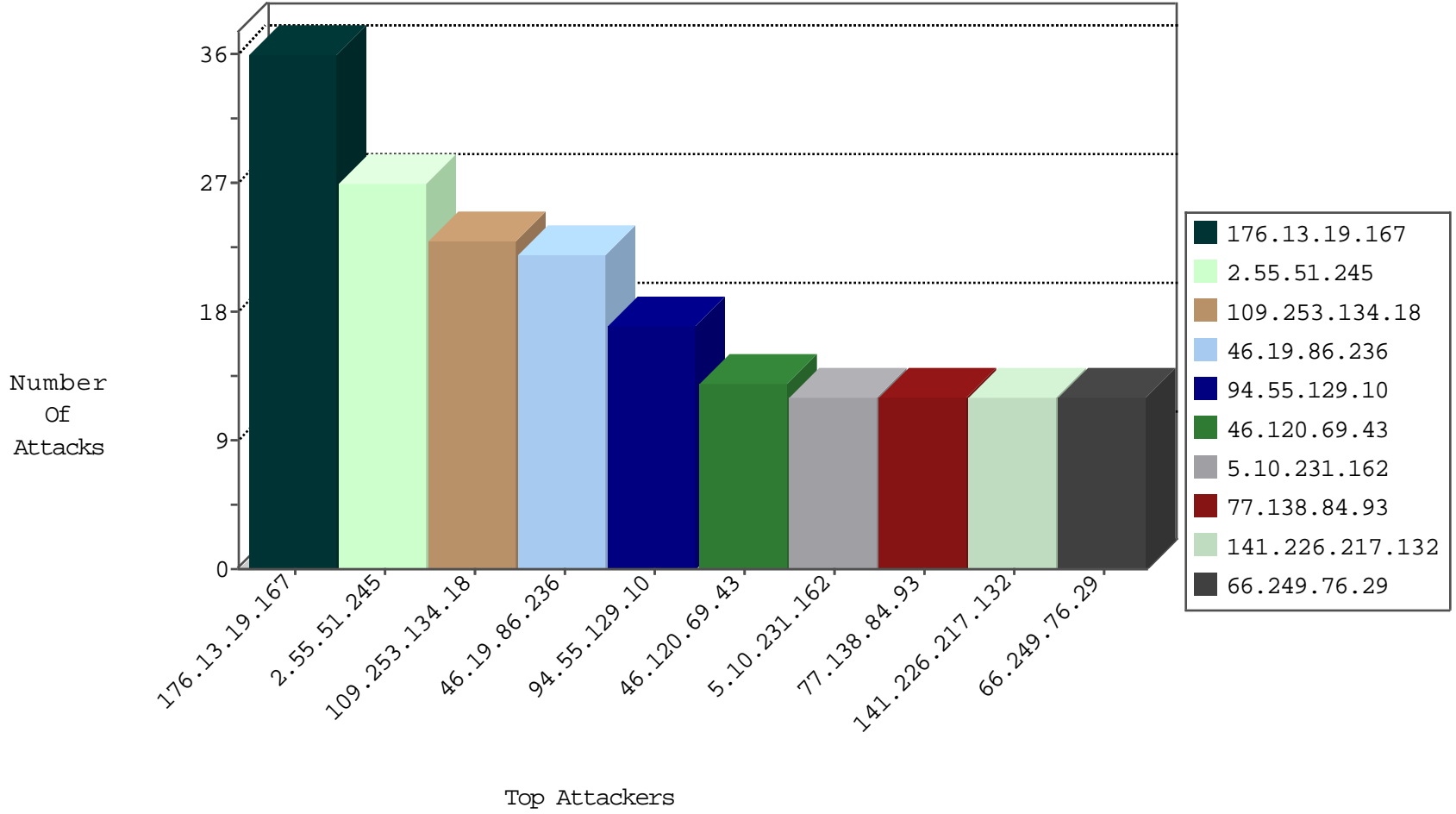
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.108.158.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13
198.44.110.15	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
198.44.110.25	United States	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.62.130	Germany	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.77.216	dover.idf.i	C1000074: HTTP: majestic bot	Permit	2
94.55.129.10	Turkey	147.237.77.216	dover.idf.i	C1000016: HTTP: administrator in URI	Permit	1
94.55.129.10	Turkey	147.237.77.216	dover.idf.i	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.182.59.140	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
213.8.204.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.155	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
85.64.222.220	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.97.58.78	147.237.76.202	Romania	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.177	Ukraine	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
81.27.85.27	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.97.58.78	147.237.76.201	Romania	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.10.231.162	Iraq	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
77.138.84.93	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
66.249.76.29	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.226.217.132	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	11
176.13.19.167	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
141.0.14.22	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	11
46.19.86.236	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.253.220.212	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.117.92.247	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.120.69.43	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
176.13.19.167	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.102.202.141	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
176.13.19.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
85.65.188.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.236	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.226	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
84.229.60.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.134.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
109.253.134.18	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.55.166.131	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
109.253.134.18	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
176.13.19.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
85.65.188.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
208.109.86.217	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.180.211.136	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.64.148	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.229.60.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
109.253.220.212	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	3
66.249.64.151	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.19.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
66.249.76.28	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.132.19	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
5.22.134.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.64.145	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.120.69.43	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.76.30	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.181.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
85.65.155.227	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.120.69.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
176.13.241.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.54.90	France	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
109.253.134.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.191.203	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.86.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.146.132	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.55.20.8	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
176.13.19.167	Israel	147.237.72.166	aka.idf.il	SYN Attack		monitor	2
109.253.195.243	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.51.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
176.13.232.201	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	8
109.253.146.83	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	7
79.179.109.240	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.179.109.240	Block	7
77.138.208.77	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/popups/	Block	5
94.55.129.10	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 94.55.129.10	Block	4
94.55.129.10	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.55.129.10	Block	4
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
94.55.129.10	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
81.140.21.209	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
77.138.97.164	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.202.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.180.211.136	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	2
77.138.87.96	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash2017/lobby.aspx	Block	2
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.66.112.162	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8892-he/refuah.aspx	Block	1
79.179.6.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/chinuch/faq/default.asp	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
81.140.21.209	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.61	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_img.asp	Block	1
87.70.240.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.11.136	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
79.179.109.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
77.138.9.5	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/yahash/sheelon.aspx	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
91.210.146.252	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/blog/	Block	1
77.139.102.104	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/gyus/	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
66.102.9.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/gyus/sitemap.aspx	Block	1
94.55.129.10	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/administrator/index.php	Block	1
66.249.73.172	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/262/trucks04102010.aspx	Block	1
2.53.181.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.55.129.10	Turkey	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
79.177.172.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachr/	Block	1