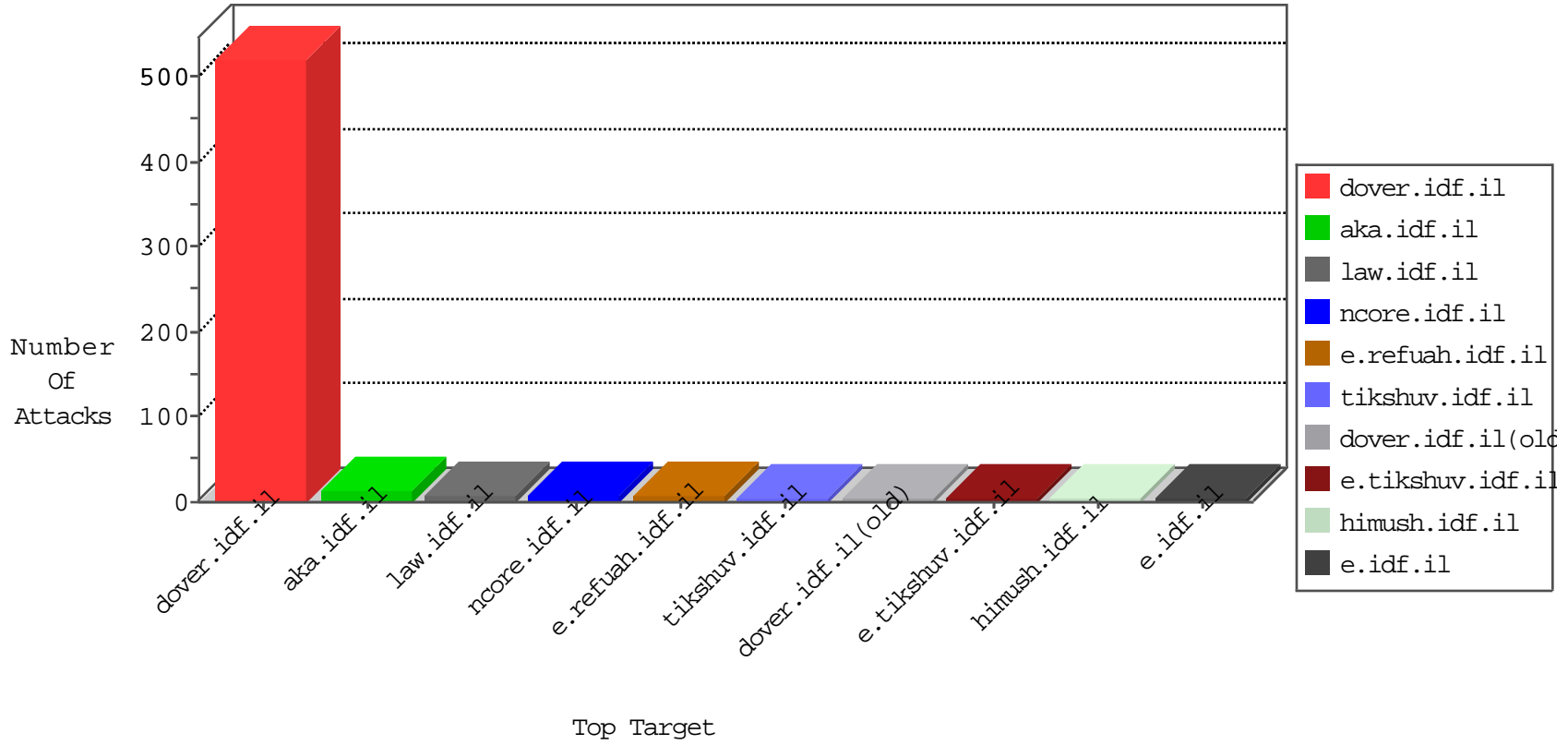
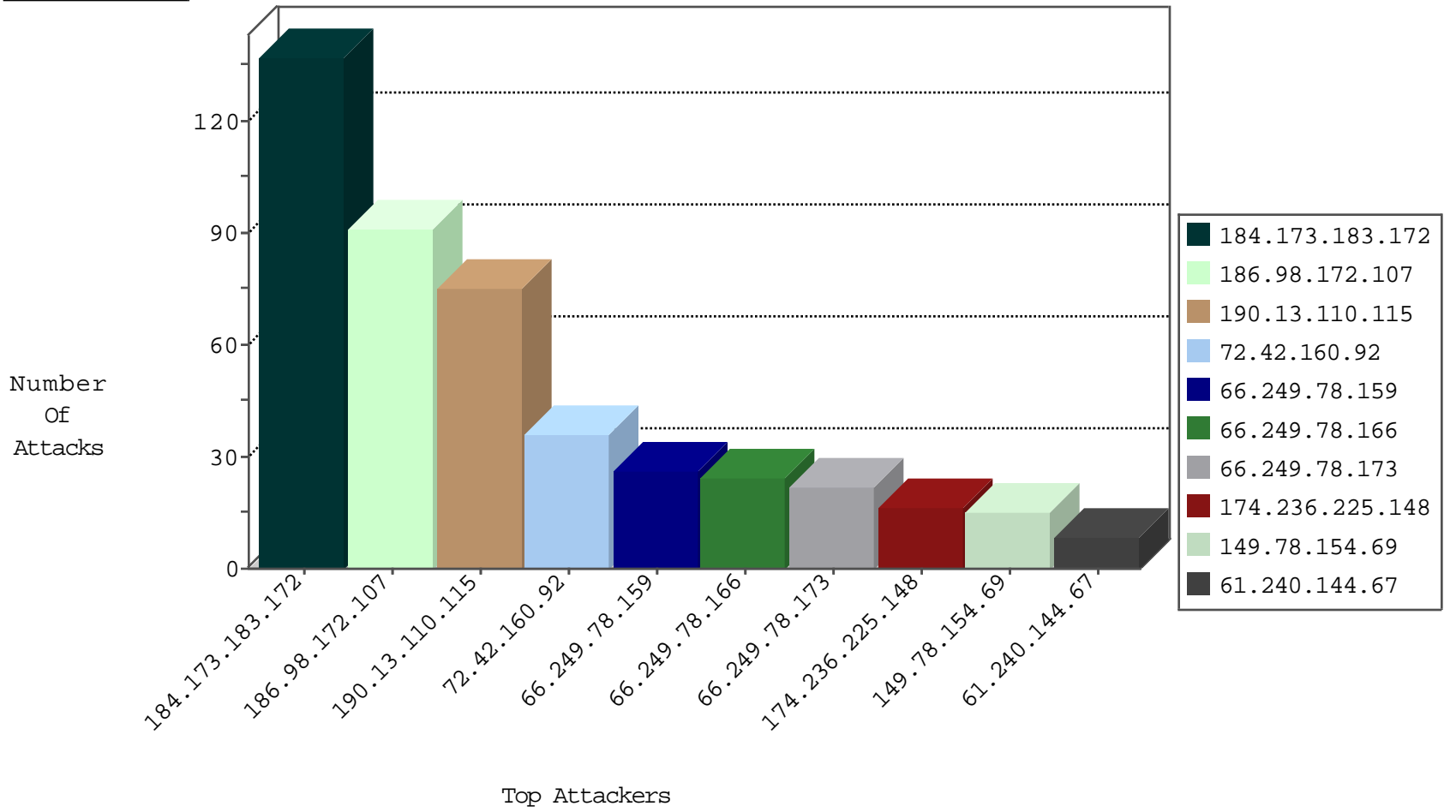


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	165
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
23.229.51.42	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
23.229.51.42	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.177	noore.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	137
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
95.90.230.91	Germany	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
79.183.56.26	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
183.136.216.3	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
178.19.107.114	Poland	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
171.34.73.180	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.89.137.3	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
171.34.73.180	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1
218.6.132.45	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
140.206.123.46	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
217.11.61.195	Germany	147.237.8.50	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
140.206.123.46	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
140.206.123.46	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
203.194.234.109	Hong Kong	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
31.13.248.97	Bulgaria	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
66.249.69.122	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
178.19.107.114	Poland	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
171.34.73.180	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
171.34.73.180	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.166	aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.6.132.45	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
171.34.73.180	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
217.116.128.15	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
140.206.123.46	China	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
140.206.123.46	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.200.91.2	Russian Federation	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
203.194.234.109	Hong Kong	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
31.13.248.97	Bulgaria	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
186.98.172.107	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	86
190.13.110.115	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	75
72.42.160.92	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
174.236.225.148	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
174.236.225.148	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	7
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
72.174.199.213	United States	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
80.179.122.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.233	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
130.211.164.37		147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.238	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
174.236.225.148	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
186.98.172.107	Colombia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
203.115.144.94	Philippines	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
70.39.157.199	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
186.98.172.107	Colombia	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
178.137.166.68	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
130.211.117.114		147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.237.138.202	Czech Republic	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
180.76.6.47	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
216.218.206.94	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
74.82.47.46	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
66.249.64.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
24.146.205.201	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
74.95.15.110	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
75.1.196.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.223.184.153	Central African Republic	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.64.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
186.98.172.107	Colombia	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1

