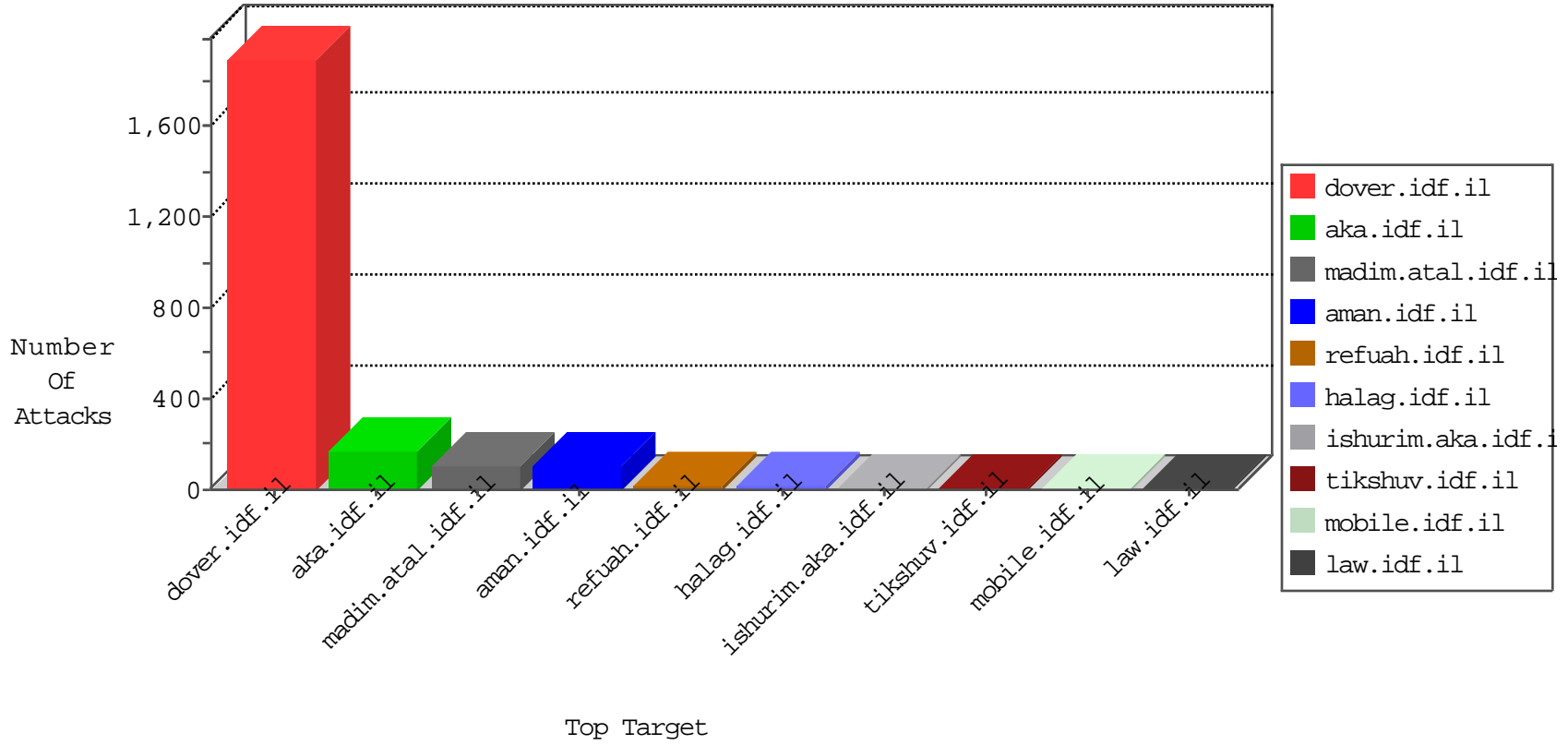
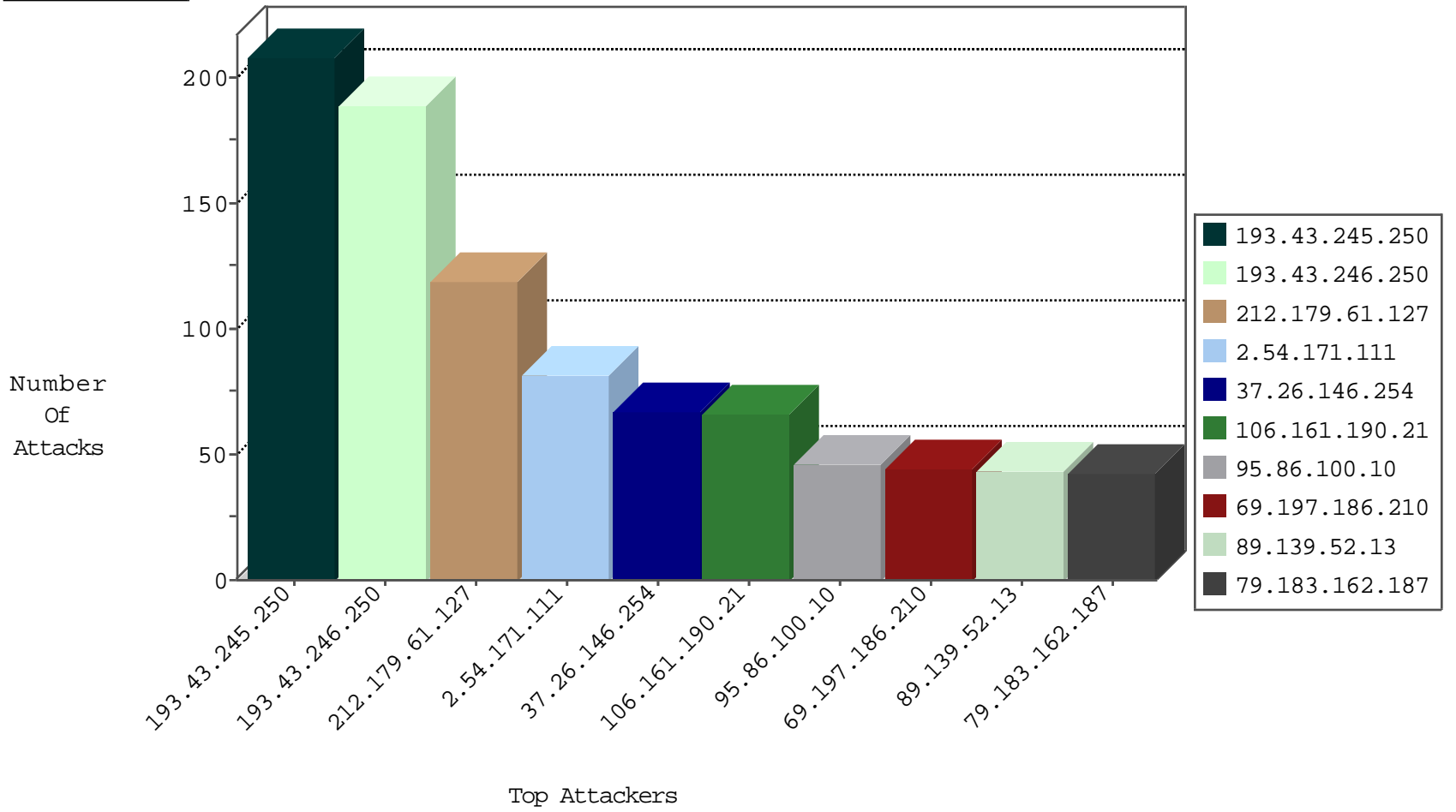




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
89.139.52.13	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	538
80.246.137.47	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
79.182.2.137	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
14.198.88.220	Hong Kong	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	4
199.203.100.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
71.6.216.56	United States	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
2.54.156.58	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
209.88.157.240	Israel	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.59	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
115.161.165.172	Korea, Republic of	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
198.48.92.104	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
69.197.186.210	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	30
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
80.178.136.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	5
85.250.135.85	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
132.66.84.121	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
46.19.85.18	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
132.64.217.88	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.142.141.215	Israel	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	2
193.105.199.1	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
85.25.103.50	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
69.114.227.252	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.201.152.245	Netherlands	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
79.183.162.187	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
69.197.186.210	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
204.83.69.189	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
5.29.91.137	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
79.178.145.187	Israel	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	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
149.88.23.43	United States	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
109.201.152.245	Netherlands	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
79.178.163.243	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.198	e.yochalan.idf.il	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	3
66.249.73.243	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.29	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	Italy	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
132.72.227.227	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
122.228.207.77	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
217.91.181.112	Germany	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
84.108.77.212	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
213.136.84.245	Germany	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
46.117.212.164	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.107	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	Italy	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
128.61.240.66	United States	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
85.65.4.158	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
217.91.181.112	Germany	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
193.43.245.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	208
193.43.246.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
212.179.61.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	116
37.26.146.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
106.161.190.21	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	66
95.86.100.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
176.44.45.48	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
95.86.111.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
54.246.252.228	Ireland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
96.242.81.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
46.19.86.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
132.71.97.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
80.179.223.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
79.178.34.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
31.168.179.2	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
79.181.200.45	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
2.54.16.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
98.248.47.127	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
69.114.227.252	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.19.115.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
207.253.174.139	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.178.163.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
62.90.101.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
197.35.68.85	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
114.109.159.72	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.144.71	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
207.46.13.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
82.80.66.122	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
192.116.190.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
73.136.136.103	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.108.90.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
2.54.148.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
84.108.21.35	Israel	147.237.77.216	dover.idf.il		drop	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
77.127.247.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
77.126.68.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
68.180.228.123	United States	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	8
109.253.146.31	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
31.44.138.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8

