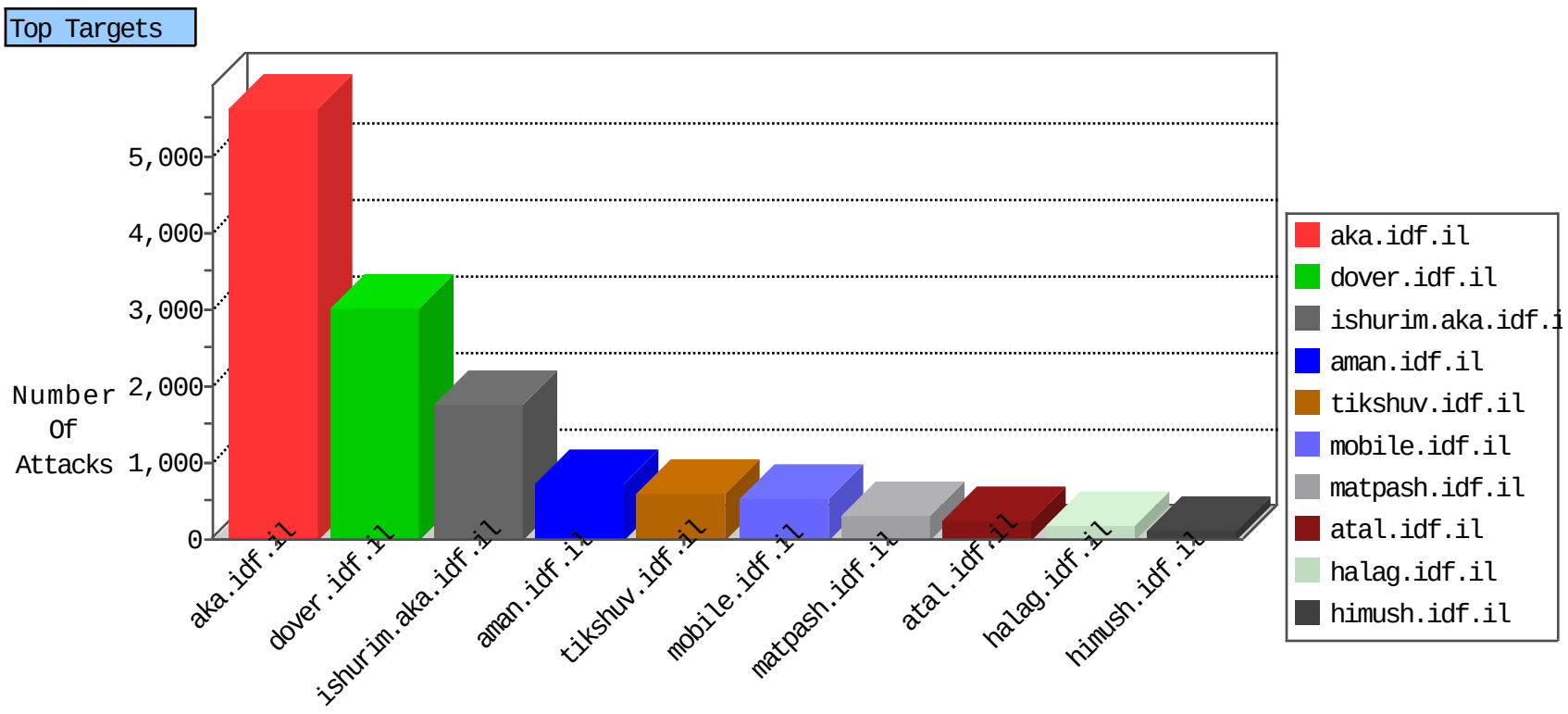
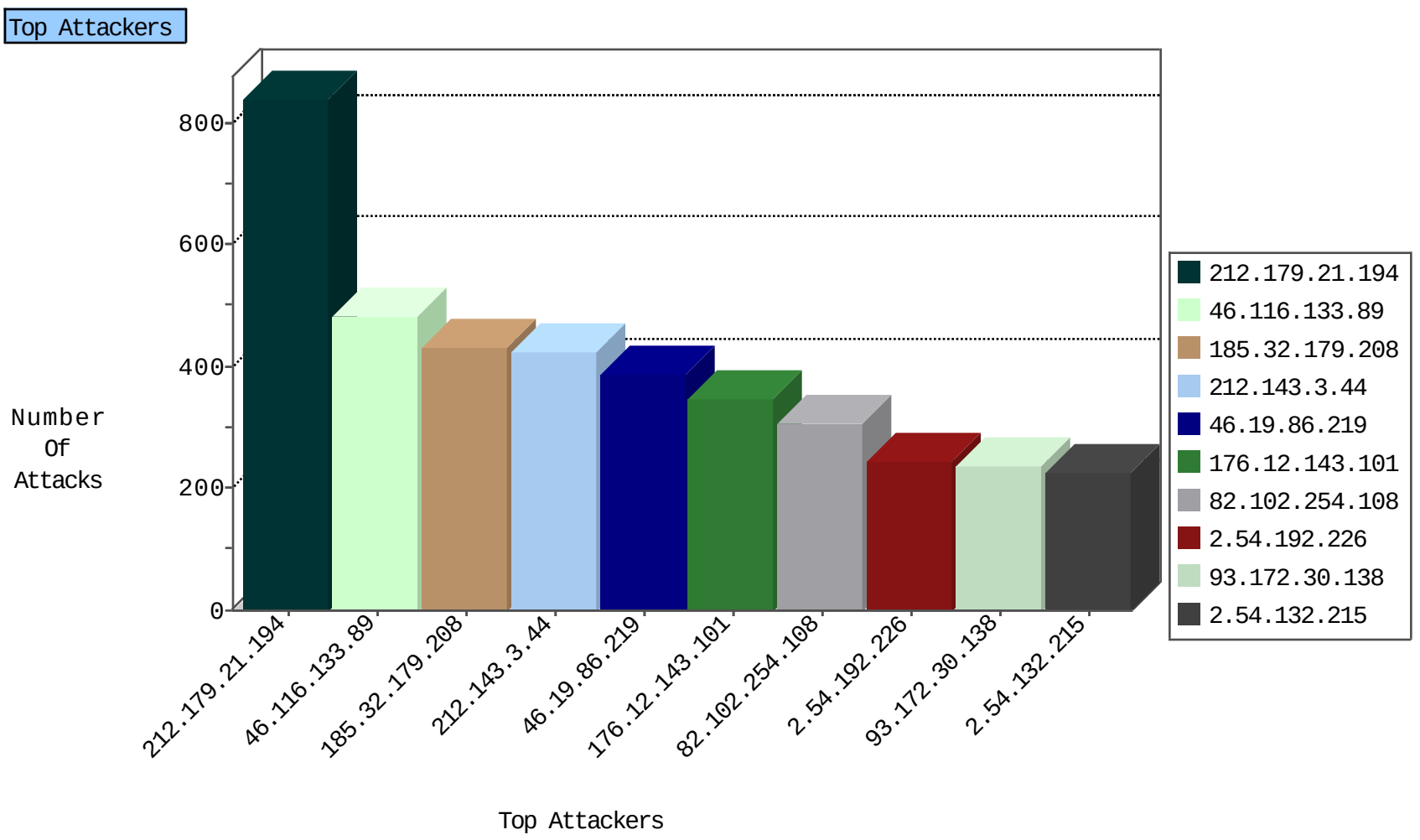
10-25-2015-12:04:09 to 10-25-2015-13:04:09

# IDF Under Attack Daily Report



10-25-2015-12:04:09 to 10-25-2015-13:04:09

Top Attackers In DDoS-Defence

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 193.106.54.34 | Israel | 147.237.77.216 | dover.idf.i | TCP handshake violation, first packet not syn | drop | 387 |
| 0.0.0.0 | | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 313 |
| 212.199.224.24 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 50 |
| 178.0.52.240 | Germany | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 22 |
| 2.54.152.253 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 16 |
| 176.12.143.101 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 16 |
| 46.103.150.207 | Greece | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 15 |
| 31.168.76.12 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 13 |
| 82.166.219.248 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 10 |
| 37.26.148.191 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 10 |
| 46.19.85.239 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 10 |
| 85.64.95.188 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 10 |
| 46.117.9.118 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 9 |
| 176.12.140.96 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 9 |
| 2.54.60.181 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 9 |
| 109.65.149.27 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 8 |
| 87.68.159.42 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 8 |
| 37.26.149.190 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 7 |
| 132.71.134.167 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 7 |
| 192.115.83.5 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 6 |
| 46.19.86.74 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 6 |
| 157.166.216.10 | United Kingdom | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 6 |
| 46.19.86.149 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 5 |
| 95.86.127.25 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 5 |
| 46.120.248.165 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 5 |
| 2.54.3.18 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 5 |
| 217.194.197.94 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 80.74.107.118 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 46.19.86.196 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 176.13.15.63 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 212.235.98.139 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 84.108.70.155 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 213.151.32.163 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 80.246.139.13 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 4 |
| 212.179.155.129 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 3 |
| 176.12.147.147 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 3 |
| 92.22.156.242 | United Kingdom | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 3 |
| 79.181.124.180 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 176.12.145.189 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 46.19.85.175 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 172.56.27.135 | United States | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 2.54.32.190 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 85.65.202.222 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 46.19.86.222 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 2.54.1.251 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 79.179.151.52 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 2 |
| 176.13.14.253 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 1 |
| 185.32.179.6 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 1 |
| 82.213.33.226 | Palestinian Territory, Occupied | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 1 |
| 80.246.136.1 | Israel | 147.237.77.216 | dover.idf.i | SYN Flood full table | drop | 1 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09

## Top Attackers In IPS

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 62.210.113.143 | France | 147.237.76.86 | navy.idf.il | 16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability | Block | 14 |
| 81.218.33.77 | Israel | 147.237.77.216 | dover.idf.i | C1000004: HTTP: options method (Microsoft) | Block | 1 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09

Top Attackers In IDS

| Attacker Address | Target Address | Attacker Country | Site | Signature | Count |
|---|---|---|---|---|---|
| 111.93.198.54 | 147.237.76.176 | India | test.ncore.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.236.96.52 | 147.237.0.200 | Germany | m4u.idf.il | ET SCAN Potential VNC Scan 5900-5920 | 1 |
| 41.33.231.90 | 147.237.77.216 | Egypt | dover.idf.il | Tehila - Perl LWP with fake user agent | 1 |
| 190.124.35.115 | 147.237.77.121 | Nicaragua | e.navy.idf.il | ET SCAN NMAP -sS window 3072 | 1 |
| 94.102.48.194 | 147.237.77.176 | Netherlands | matpash.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 77.236.96.52 | 147.237.0.200 | Germany | m4u.idf.il | ET SCAN NMAP -sS window 1024 | 1 |
| 190.124.35.115 | 147.237.77.121 | Nicaragua | e.navy.idf.il | ET SCAN NMAP -sS window 4096 | 1 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09

## Top Attackers In FW

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 212.179.21.194 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 765 |
| 185.32.179.208 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 433 |
| 212.143.3.44 | Israel | 147.237.0.34 | tikshuv.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 419 |
| 46.116.133.89 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 355 |
| 46.19.86.219 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 325 |
| 176.12.143.101 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 309 |
| 82.102.254.108 | Palestinian Territory, Occupied | 147.237.77.176 | matpash.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 299 |
| 93.172.30.138 | Israel | 147.237.77.233 | atal.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 233 |
| 2.54.132.215 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 225 |
| 79.177.226.15 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 204 |
| 2.54.134.154 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 198 |
| 79.179.209.40 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 197 |
| 192.118.64.29 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 184 |
| 87.68.160.121 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 181 |
| 2.54.192.226 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 177 |
| 176.228.165.201 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 171 |
| 79.181.60.244 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 166 |
| 46.19.85.196 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 164 |
| 194.90.122.40 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 163 |
| 37.19.117.217 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 157 |
| 46.117.9.118 | Israel | 147.237.77.234 | halag.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 147 |
| 192.115.83.5 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 147 |
| 62.219.177.130 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 144 |
| 95.86.114.158 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 140 |
| 79.180.37.18 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 137 |
| 146.185.58.66 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 136 |
| 195.200.205.2 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 130 |
| 176.13.23.51 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 130 |
| 109.186.53.74 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 127 |
| 82.80.196.44 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 126 |
| 46.116.133.89 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 126 |
| 149.78.14.230 | Israel | 147.237.76.30 | himush.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 125 |
| 109.66.41.171 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 124 |
| 176.13.16.28 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 120 |
| 79.181.162.208 | Israel | 147.237.77.216 | dover.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 117 |
| 85.64.179.81 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 109 |
| 46.19.86.237 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 102 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09

| Attacker Address | Attacker Country | Target Address | Site | Signature | Message | Device Action | Count |
|---|---|---|---|---|---|---|---|
| 79.183.38.152 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 99 |
| 62.90.88.104 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 98 |
| 79.176.25.15 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 97 |
| 46.19.86.5 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 94 |
| 31.168.126.214 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 92 |
| 176.12.139.209 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 90 |
| 91.199.69.254 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 86 |
| 46.19.85.132 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 86 |
| 82.81.240.47 | Israel | 147.237.72.167 | ishurim.aka.idf.i | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 86 |
| 176.13.18.7 | Israel | 147.237.77.243 | mobile.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 85 |
| 2.54.40.194 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 84 |
| 91.135.102.163 | Israel | 147.237.72.156 | aman.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 80 |
| 149.78.95.253 | Israel | 147.237.72.166 | aka.idf.il | Streaming Engine: TCP Segment Limit Enforcement | TCP segment out of maximum allowed sequence. Packet dropped. | drop | 80 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09

## Top Attackers In WAF

| Attacker Address | Attacker Country | Target Address | Site | Signature | Device Action | Count |
|---|---|---|---|---|---|---|
| 79.181.26.35 | Israel | 147.237.76.42 | refuah.idf.i | Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx | Block | 14 |
| 2.54.192.226 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 14 |
| 31.168.23.67 | Israel | 147.237.77.216 | dover.idf.il | Unauthorized URL Access to www.idf.il/bamahane | Block | 14 |
| 46.19.86.231 | Israel | 147.237.72.166 | aka.idf.il | Untraceable SSL Sessions: Open Mode | None | 14 |
| 66.249.78.253 | Israel | 147.237.72.156 | aman.idf.il | Unauthorized URL Access to list.ips.gov.il/ | Block | 14 |

10-25-2015-12:04:09 to 10-25-2015-13:04:09