Peakflow® SP Threat Management System

Threat analysis, surgical mitigation and service protection

Internet service providers (ISPs), cloud providers and enterprises face a common problem. Distributed denial of service (DDoS) attacks are a major risk to service availability. The power, sophistication and frequency of DDoS attacks are rising. Data center operators and network providers need a defense that is effective, cost-efficient and easily managed. Arbor’s Peakflow SP Threat Management System ("Peakflow SP TMS") is the acknowledged leader in DDoS protection. More service providers, cloud providers and large enterprises use Peakflow SP TMS for DDoS mitigation than any other solution.

Peakflow SP Solution for DDoS Protection

The Peakflow SP ("Peakflow SP") solution integrates network-wide intelligence and anomaly detection with carrier-class threat management to identify and stop network and application-layer DDoS attacks.

Peakflow SP TMS network appliances provide the vital, traffic-scrubbing component of the Peakflow SP solution. Peakflow SP TMS can be deployed inline to provide "always on" protection. Unlike other products, it also supports a mitigation architecture called "diversion/reinjection." In this mode, only the traffic stream carrying the DDoS attack is redirected to Peakflow SP TMS through routing updates issued by the Peakflow SP solution. Peakflow SP TMS removes only the malicious traffic from that stream and forwards the legitimate traffic to its intended destination.

This is highly advantageous for service providers, large enterprises and large hosting/cloud providers. It enables a single, centrally located Peakflow SP TMS to protect multiple links and multiple data centers. It results in much more efficient use of mitigation and fully non-intrusive security. Inline devices must inspect all traffic all the time on the links they monitor. Peakflow SP TMS only needs to inspect traffic that is redirected to it in response to an attack on a specific target.

Key Features and Benefits

**Surgical Mitigation**
Automatically remove only the attack traffic without interrupting the flow of legitimate business traffic.

**Unified Command and Control of Two Tb of Global Mitigation**
Scale DDoS defenses to an unprecedented level. Deploy up to two terabits of aggregate, centrally managed mitigation capacity.

**Managed Services Enabler**
Meet rapidly growing demand for DDoS protection services. Use Peakflow SP TMS to deliver profitable managed security services.

**Service Protection and Application Intelligence**
Maintain service levels of your most important applications. Monitor performance and protect applications from targeted attacks.

**Flexible Deployment**
Deploy application-layer intelligence, threat detection and surgical mitigation in different portions of your network for infrastructure protection and profitable managed services.

Comprehensive threat detection and surgical mitigation
**Multiple Methods of Threat Detection and Mitigation**

**Block known malicious hosts** by using white and black lists. The white list contains authorized hosts, while the black list contains zombies or compromised hosts whose traffic will be blocked.

**Block application-layer exploits** by using complex filters. Peakflow SP TMS provides payload visibility and filtering to ensure cloaked attacks cannot bring down critical services.

**Defend against Web-based threats** by detecting and mitigating HTTP-specific attacks. These mechanisms also help with managing flash-crowd scenarios.

**Protect critical DNS services** from cache poisoning, resource exhaustion and amplification attacks. Add greater visibility into DNS services.

**Protect VoIP services** from automated scripts or botnets that exploit packet-per-second and malformed request floods by employing VoIP/SIP-specific attack detection and mitigation capabilities.

**Control the zombie army** by using specialized, always-on and learning zombie detection mechanisms that ensure compromised hosts are not attacking mission-critical infrastructure.

**Protect SSL-based services** (Web, email, file transfer) from attacks on SSL protocols and infrastructure.

---

### ATLAS® Intelligence Feed (AIF)

Leveraging a global network of traffic monitoring and sensors, Arbor researchers have developed AIF, a library of targeted defenses providing automatic protection from the vast majority of botnet-based attacks. AIF automatically updates Peakflow SP TMS with new protections as Arbor researchers find and neutralize emerging threats.

---

### Comprehensive Threat Detection

Data centers and public networks present multiple targets for DDoS attacks. These targets include infrastructure devices (e.g., routers, switches and load balancers), domain name systems (DNS), bandwidth capacity and key applications such as Web, ecommerce, voice and video. Even security devices such as firewalls are targets of attack. The Peakflow SP solution provides the most comprehensive and adaptive suite of threat detection capabilities in the industry, designed to protect diverse resources from complex, blended attacks. These capabilities include statistical anomaly detection, protocol anomaly detection, fingerprint matching and profiled anomaly detection. Peakflow SP continually learns and adapts in real time, alerting operators to attacks as well as to unusual changes in demand and service levels.

### Surgical Mitigation

Key to effective mitigation is the ability to identify and screen attack traffic while allowing legitimate traffic to flow through to its intended destination. Large-scale DDoS attacks affect not only the intended victim, but also other unfortunate customers who may be using the same shared network service. To reduce this collateral damage, service providers and hosting providers often shut down all traffic destined for the victim’s site, thus completing the DDoS attack. Whether it’s a high-volume flood attack designed to exhaust bandwidth capacity or a targeted attack looking to bring down a Web site, Peakflow SP TMS can isolate and remove the attack traffic without affecting legitimate users. Methods include identifying and black-listing malicious hosts, IP location-based mitigation, protocol anomaly-based filtering, malformed packet removal and rate limiting (to gracefully manage non-malicious demand spikes). Mitigations can be automated or operator-initiated and countermeasures can be combined to address blended attacks.

---

### Real-Time Mitigation Dashboard

The Peakflow SP TMS real-time mitigation dashboard is a single screen that shows operators exactly what is generating a DDoS alert and what effect the countermeasures are having on the attack. It provides the ability to modify countermeasures and delivers full packet capture and decode to get a detailed view of both legitimate and attack packet streams. This information is stored for future reference and management reporting—giving operators and managers full visibility and reporting into attacks on their business operations.

### Flexible Deployment, Rapid Enablement

Configuration templates and out-of-the-box mitigation enable operators to implement effective DDoS defense from day one. Peakflow SP TMS automatically learns normal traffic patterns and adjusts over time, eliminating the need to manually configure and update alert thresholds. Operators also have the option to set thresholds and manually initiate mitigations. In short, Peakflow SP TMS allows operators to choose how much they wish to automate and how much they wish to control manually.
Comprehensive Management and Reporting

Peakflow SP TMS simplifies and streamlines operations by providing the ability to view and manage up to two terabits of mitigation capacity from a single point of control. This provides the ability to thwart multiple, large-scale attacks and produce comprehensive reports that summarize the mitigation process for customers and/or management.

A Platform for Managed DDoS Services

Arbor’s Peakflow SP solution enables service providers and hosting/cloud providers to deliver DDoS protection services. Customized portal access, APIs and delegated management give managed services providers the flexibility and control to tailor services to fit their customers’ needs. Peakflow SP is the undisputed leader for managed DDoS protection. It is the solution of choice for the vast majority of leading DDoS managed services.

Peakflow SP TMS 1200, 2500, 3050 and 3110 Specifications

<table>
<thead>
<tr>
<th>Power Requirements</th>
<th>1200</th>
<th>Redundant Dual Power Supplies; AC: 100-127V/200-240V, 50 to 60Hz, 4/2A; DC: -48 to -60V, 7A max</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2500</td>
<td>Redundant Dual Power Supplies; AC: 100-127V/200-240V, 50 to 60Hz, 6/3A; DC: -48 to -60V, 10A max</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>Redundant Dual Power Supplies; AC: 100-240V, 50 to 60Hz, DC: -40 to -72V</td>
</tr>
<tr>
<td>Dimensions</td>
<td>1200</td>
<td>Chassis: 1U rack height; Weight: 25.41 lb (11.52 kg); Height: 1.7 inches (4.22 cm); Width: 16.93 inches (43 cm); Depth: 20 inches (51 cm)</td>
</tr>
<tr>
<td></td>
<td>2500</td>
<td>Chassis: 2U rack height; Weight: 39 lb (17.2 kg); Height: 3.45 inches (8.76 cm); Width: 17.14 inches (43.54 cm); Depth: 20 inches (51 cm)</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>Chassis: 3U rack height; Weight: 93.5 lbs (42.5 kg); Height: 5.25 inches (13.34 cm); Width: 17.63 inches (44.8 cm); Depth: 16.28 inches (41.33 cm)</td>
</tr>
<tr>
<td>Network Interfaces, Hard Drive</td>
<td>1200</td>
<td>4 x 10/100/1000 (fiber GigE SX and LX available) Dual Hard Drive RAID 1</td>
</tr>
<tr>
<td></td>
<td>2500</td>
<td>6 x 10/100/1000 (fiber GigE SX and LX available) Dual Hard Drive RAID 1</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>2 x 10 GigE (SFP+) 10 x 1 GigE (SFP) Dual Hard Drive RAID 1</td>
</tr>
<tr>
<td>Environmental</td>
<td>1200, 2500</td>
<td>Operating temperature: 41°F to 104°F (5°C to 40°C); Relative humidity (operating): 5 to 85%, (non-operating): 93% at 73°F to 104°F (23°C to 40°C)</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>Operating temperature: 23°F to 131°F (-5°C to 55°C); Relative humidity (operating): 5 to 95% non-condensing</td>
</tr>
<tr>
<td>Regulatory</td>
<td>1200</td>
<td>RoHS, IEC 60950-1 2nd ed., FCC Part 2, FCC Part 15 Subpart B Class A, EN 55022 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3, ETI EN 300 386, CISPR 22 Class A, CISPR 24, CCO, Gost, BSMI, VCCI Class A, KCC RLL, C-Tick, MIC, CD, UL Mark, CE Mark</td>
</tr>
<tr>
<td></td>
<td>2500</td>
<td>RoHS, IEC 60950-1 1st ed., FCC Part 2, FCC Part 15 Subpart B Class A, EN 55022 Class A, EN 55024, EN 61000-3-2, EN 61000-3-3, ETI EN 300 386, CISPR 22 Class A, CISPR 24, ACC, Gost, BSMI, VCCI Class A, KCC RLL, C-Tick, UL Mark, CE Mark, ETI, NEBS-3</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>RoHS 6/6, IEC/EN/UL 60950-1, FCC Part 15 Subpart B Class A, ETI EN 300 386, UL Mark, CE Mark</td>
</tr>
<tr>
<td>Hardware Bypass</td>
<td>1200, 2500</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>3050, 3110</td>
<td>External</td>
</tr>
<tr>
<td>Throughput</td>
<td>1200</td>
<td>1.5 Gbps, 500K pps</td>
</tr>
<tr>
<td></td>
<td>2500</td>
<td>2.5 Gbps, 1M pps</td>
</tr>
<tr>
<td></td>
<td>3050</td>
<td>5 Gbps, 2M pps</td>
</tr>
<tr>
<td></td>
<td>3110</td>
<td>10 Gbps, 4M pps</td>
</tr>
</tbody>
</table>
Peakflow SP TMS 1200
1.5 Gbps, 500K pps

Peakflow SP TMS 2500
2.5 Gbps, 1M pps

Peakflow SP TMS 3050
5 Gbps, 2M pps

Peakflow SP TMS 3110
10 Gbps, 4M pps

Peakflow SP TMS 4000
10 Gbps, 10M pps – 40 Gbps, 40M pps

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe
T +44 207 127 8147

Asia Pacific
T +65 6299 0695

www.arbornetworks.com

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including the vast majority of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 230+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.