[DATA SHEET]

Arbor Peakflow SP

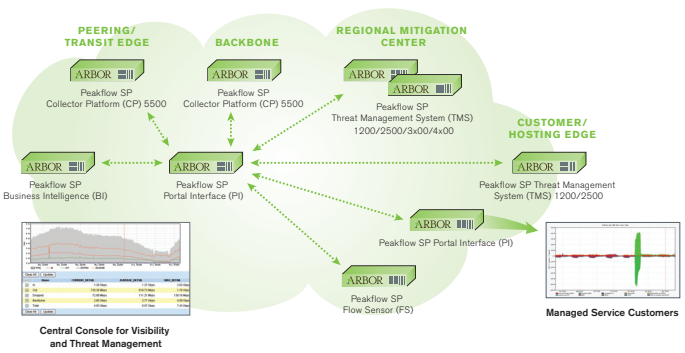
PERVASIVE NETWORK VISIBILITY, SECURITY AND MANAGED SERVICES

Internet service providers (ISP), application/hosting service providers (ASP) and large enterprises all face the challenge of delivering high quality services and high availability at a reasonable cost. With traffic volumes constantly increasing and the added complexity of supporting both IPv4 and IPv6, meeting these challenges is more difficult than ever. Arbor Networks understands this. The Arbor Peakflow SP solution ("Peakflow SP") is a network-wide infrastructure security and traffic-monitoring platform. The cost-efficient, comprehensive security and traffic monitoring capabilities of Peakflow SP provide key elements of availability assurance. As the de facto security standard for the majority of the world's leading service providers, Peakflow SP monitors and protects over 70% of today's global Internet traffic.

Knowledge Is Power

Arbor Peakflow SP is a solution for network-wide, non-intrusive reporting, anomaly detection and intelligent mitigation. Using flow data, SNMP and BGP updates, Peakflow SP learns normal traffic and routing behavior across hundreds of routers and thousands of interfaces, and correlates the traffic patterns with the topology data to build logical data models. This information enables network and security operations staff to detect and mitigate threats to availability, improve network/service performance and make better investment decisions concerning capacity planning, service offerings and traffic management. Peakflow SP is based on the following principles:

- **Know Your Network:** Pervasive visibility into network, application and routing traffic allows you to make sound decisions about transit partners, network architecture, customers and new IP services.
- **Secure Your Network:** Real-time detection, mitigation and comprehensive reporting of security events enable you to minimize their adverse impact on your network, your services and your customers.
- **Grow Your Network:** Leverage the same Arbor Peakflow SP platform used for network visibility and security to deliver differentiated, profitable, in cloud distributed denial of service (DDoS) managed services.



Peakflow SP Architecture

Consists of five types of appliances: 1) Peakflow SP Collector Platform (CP) appliances in the peering edge or backbone; 2) Peakflow SP Flow Sensor (FS) appliances in the customer aggregation edge; 3) Peakflow SP Business Intelligence (BI) appliances to increase scalability and add redundancy for managing critical business objects; 4) Peakflow SP Portal Interface (PI) appliances to increase the scale, redundancy and profitability of Arbor-based managed services; and 5) Peakflow SP Threat Management System (TMS) appliances deployed in any part of the network to surgically mitigate network threats.

Key Features and Benefits

Protect Services

Safeguard critical services such as voice, video, Web, ecommerce and email from targeted attacks.

Protect Infrastructure

Detect and remove attacks on routers, switches, firewalls, bandwidth and DNS services. Keep illegitimate traffic off the network.

Maintain Performance

Gain visibility into key application performance metrics such as jitter, latency, round-trip time, delay and packet loss. Spot problems and take action before users start to complain.

Optimize Resources

Use traffic visibility and comprehensive reports for better traffic engineering and faster, more effective troubleshooting. Reduce transit costs, improve utilization and intelligently plan for growth.

Launch Managed Services

Leverage the same Arbor Peakflow SP platform used for network visibility and security to easily provision, deliver and maintain differentiated, profitable, in-cloud DDoS managed services.

ARBOR NETWORKS

Real-Time Global Threat Analysis—From One Console

The Arbor Security, Engineering and Response Team (ASERT) leverages Arbor's trusted relationship with a majority of the world's Internet service providers to gain unique insight into global threat activity. As a result, ASERT delivers multiple benefits back to the industry and Arbor customers under a broad initiative know as the Active Threat Level Analysis System (ATLAS). Below are some of the ATLAS deliverables that manifest themselves in the Peakflow SP solution:

ATLAS Security Portal

The ATLAS security portal (located at atlas.arbor.net) provides a real-time view into global threat activity. This information is easily accessible from within the Peakflow SP console, allowing service providers to see how worldwide threat activity may be impacting their network.

Fingerprints

As ASERT analyzes global threat activity, it creates "fingerprints" that are the network behavioral patterns of attacks. These fingerprints are automatically distributed to Peakflow SP customers via the Active Threat Feed (ATF) service—allowing Peakflow SP TMS to detect and surgically mitigate attacks that match these fingerprints.

Fingerprint Sharing Alliance

The distributed nature of DDoS attacks requires ISPs to work with each other to stop these events. To help facilitate this collaboration, Arbor created the Fingerprint Sharing Alliance (FSA), which allows services providers to easily share fingerprints among their Peakflow SP deployments.

Cloud Signaling

Arbor's latest advance in DDoS defense provides automated and coordinated response to attacks that threaten to both overwhelm network bandwidth capacity and data center services.

The Power, Scalability and Availability You Need

As networks grow and traffic volumes increase, a key attribute of any monitoring and security solution is the ability to scale. From a single management console the Peakflow SP solution gives operators visibility across the largest networks and unified command and control of up to 2 terabytes of DDoS mitigation capacity. Peakflow SP does not require operators to install additional probes, network taps and inline devices. The flexibility to accept multiple flow and data formats enables Peakflow SP to be used in a wide variety of network environments.

Comprehensive and Reliable DDoS Defense

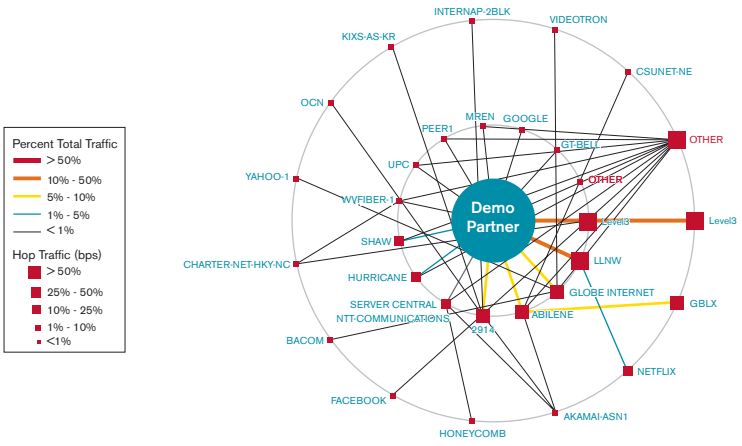
The number one threat to IP-service availability is DDoS. Peakflow SP defends against attacks that seek to exhaust bandwidth, as well as targeted application-layer attacks on business-critical IP services such as domain name system (DNS), HTTP and Voice over Internet Protocol (VoIP). The proven Ability of Peakflow SP to detect sophisticated, blended attacks, combined with its comprehensive suite of mitigation options, enables operators to successfully screen attack traffic while allowing legitimate users to fully access services. Peakflow SP is the most widely deployed and trusted solution for DDoS protection.

Meet the Challenge of Pervasive Change

With the introduction of IPv6, DNSSEC and 4 Byte ASNs, networks and data centers are entering a period of pervasive change that will impact almost every aspect of operations. Now more than ever, operations staff need comprehensive network visibility and DDoS protection to ensure availability and to control costs. Peakflow SP protects networks from new DDoS attack vectors and enables operators to make informed traffic engineering decisions that save money.

Intelligent Traffic Engineering, Capacity Planning and Troubleshooting

Peakflow SP provides detailed visibility into IPv4 and IPv6 traffic, Border Gateway Protocol (BGP) routing, Multiprotocol Label Switching virtual private networks (MPLS VPNs), quality of service (QoS) and applications including DNS, VoIP and peer-to-peer (P2P). This enables network operators to recognize and correct service-impacting issues in real time, as well as improve traffic engineering and capacity planning.



Peering analysis report–Reduce transit costs

Service Visibility, Performance and Protection

From a user perspective, the network is only as good as the applications and IP services that run on it. The diversity of customer applications, ranging from triple-play services (e.g., data, voice and video) to over-the-top (OTT) applications (e.g., IM, Skype™ and YouTube™) makes service optimization even more challenging. Using flow and payload analyses, Peakflow SP and the Arbor Peakflow Threat Management System ("TMS") automatically recognize over 90 applications and provide the ability to specify custom applications for monitoring. To help ensure customer satisfaction and optimal performance of applications such as HTTP, VoIP and DNS, Peakflow SP and TMS provide insight into key metrics such as jitter, latency, network round-trip times, delay and packet loss.

Advanced Reporting and Management

Peakflow SP provides the industry's most comprehensive and flexible reporting and management system for network visibility and security. It is designed for use in multiple contexts—including enterprise, hosting provider and service provider environments.

Features include the ability to monitor, report and protect up to 10,000 managed objects (e.g., customers, IP address ranges, interfaces, routes and services), extensive reporting and drill-down capability, report customization, reporting API, plus the definition of flexible and customizable management roles.

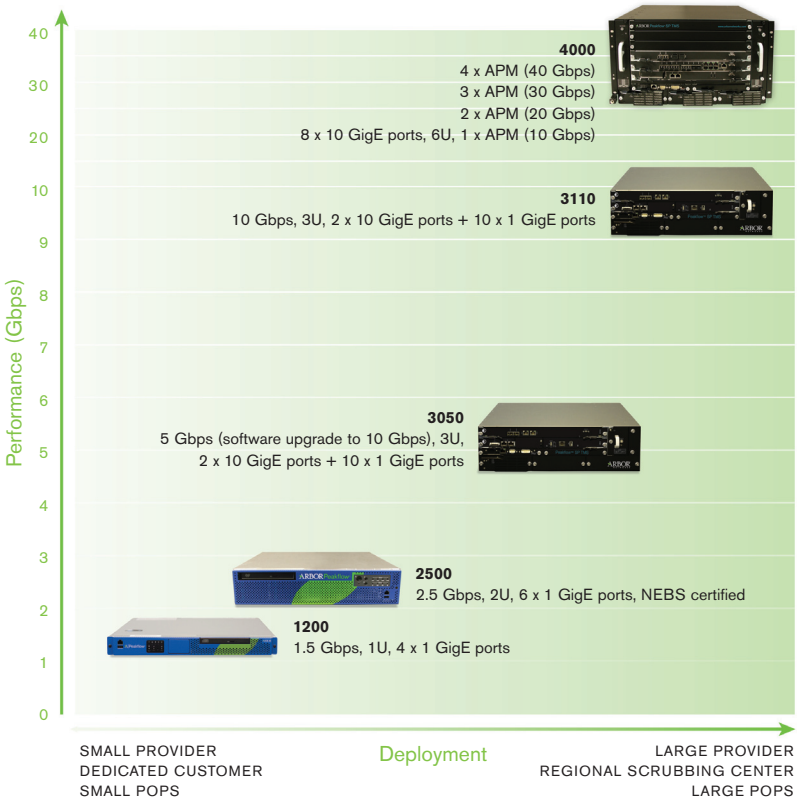
The Solution for Profitable Managed DDoS Services

Peakflow SP reduces the operational complexity and cost of deploying a managed DDoS service. Key features include templates/APIs for customized portals, redundancy, automated failover, data synchronization, "one-click" or auto-mitigation, customizable mitigation templates, real-time mitigation dashboards and comprehensive mitigation reports. These features simplify the provisioning and operational support of the managed DDoS service—increasing profitability and customer satisfaction.

Arbor Peakflow SP TMS plays a vital role in a Peakflow SP-based managed DDoS service. TMS is an application-intelligent appliance for multi-service converged networks that speeds remediation by coupling high-level threat identification with packet-level analysis. TMS allows providers to detect network and application-layer attacks and surgically scrub only the attack traffic while allowing non-attack traffic.

Optimized DDoS Protection

To optimize the deployment of DDoS mitigation, Peakflow SP TMS offers a variety of models and feature sets. The chart below outlines the various models, their features, performance capabilities and deployment scenarios.



Peakflow SP TMS deployment

Multiple Methods of Threat Detection and Mitigation

The combination of Peakflow SP and Peakflow SP TMS allows service providers to protect critical IP services by leveraging the following methods of attack/anomaly 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 prevent cloaked attacks from bringing down critical services.

Defend against Web-based threats or anomalies by using mechanisms to detect and mitigate HTTP-specific attacks. These mechanisms also help with managing flash-crowd scenarios.

Shield DNS services from botnets that mask, amplify and deliver exploits to DNS infrastructure and services. Arbor Peakflow solutions enable you to employ DNS-specific attack detection and mitigation capabilities.

Protect critical VoIP services from automated scripts or botnets that exploit packet per second and malformed request floods. Arbor Peakflow solutions enable you to employ VoIP/SIP-specific attack detection and mitigation capabilities.

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

Enforce baseline protection by building ongoing, always learning models of network behavior. This information can be leveraged to identify abnormal traffic and block it from the network at the time of attack.

"We've been growing with the Peakflow product set since the beginning when we were a small ISP to now as a global service provider. Working with Arbor has been an absolute pleasure over the last five years. I would not hesitate recommending the product to anyone who runs an IP network—either on a local or global scale."

Christiaan Keet, Network Services Director, Easynet Global Services

Peakflow SP Appliances

Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI) and Portal Interface (PI). Each utilizes the depicted enclosure.

ARBOR NETWORKS

Corporate Headquarters

6 Omni Way
Chelmsford, Massachusetts 01824

Toll Free USA +1 866 212 7267
T +1 978 703 6600
F +1 978 250 1905

Europe

T +44 208 622 3108

Asia Pacific

T +65 6299 0695

www.arbornetworks.com

DS/SP/EN/0611

Arbor Peakflow SP Collector Platform (CP), Flow Sensor (FS), Business Intelligence (BI) and Portal Interface (PI) Appliance Specifications

Power Requirements
Redundant dual power sources
AC: 100 to 240V (50-60 Hz),
DC: -38 to -75V

Physical Dimensions
Chassis: 2U rack height
Weight: 39 lbs (17.7 kg)
Height: 3.45 in (8.76 cm)
Width: 17.4 in (43.53 cm)
Depth: 20 in (51 cm)
Standard 19 in and 23 in rack mountable

Hard Drives
Four hard drives running RAID 5

NICs
2 x 10/100/1000BaseT (fiber option available)

Environmental
Operating: 32° to 104°F (0° to 40°C)
Relative Humidity (Non-Operating): 95%, non-condensing at temperatures of 73° to 104°F (23° to 40°C)

Operating System
ArbOS®/ArbUX, our proprietary, embedded operating systems, are based on open source operating system technology such as Linux and Open BSD.

Performance
Configured for NetFlow (OC-48) and packets (GigE)

Compatibility
Flow Data: Supports Cisco NetFlow v5, v7, v9; sFlow Juniper cflowd, jFlow, IPFix, Netstream v9
Monitoring: Integrates with management consoles supporting SNMP v3
Web-Based UI: IE 7.0, 8.0 on Windows XP, Vista, Windows 7 and Mozilla Firefox 3.5, 3.6 on Windows XP, Vista, Windows 7, Mac OSX

Regulatory Compliance
ETSI, NEBS and RoHS compliant

Arbor Peakflow SP TMS Specifications

Power Requirements
Redundant dual power sources

4000
AC: 100/240V, 50-60Hz, circuit amp 20A
DC: -48 to -68V, circuit amp 50A, 380-980W nominal, 1200-1650W max

3050/3110
AC: 100/240V, 50-60Hz, 460W nominal, 500W max, circuit amp 20A
DC: -48 to -68V, 460W nominal, 600W max, circuit amp 20A

2500
AC: 100/240V, 50-60 Hz, circuit amp 15A, 600W max
DC: -48 to -60V

1200
AC: 100/240V, 50-60 Hz, circuit amp 15A; 450W max
DC: -48 to -60V, circuit amp 15A; 450W max

Physical Dimensions
Standard 19 in and 23 in rack mountable

4000
Chassis: 6U rack height
Weight: 85.3 lbs (38.7 kg)
Height: 10.5 in (26.7 cm)
Width: 17.64 in (44.8 cm)
Depth: 16.3 in (41.4 cm)

3050/3110
Chassis: 3U rack height
Weight: 33.5 lbs (15.2 kg)
Height: 5.25 in (13.34 cm)
Width: 17.64 in (44.8 cm)
Depth: 16.28 in (41.33 cm)

2500
Chassis: 2U rack height
Weight: 39 lbs (17.7 kg)
Height: 3.45 in (8.76 cm)
Width: 17.11 in (43.46 cm)
Depth: 20 in (51 cm)

1200
Chassis: 1U rack height
Weight: 25.41 lbs (11.52 kg)
Height: 1.7 in (4.32 cm)
Width: 16.93 in (43 cm)
Depth: 20 in (51 cm)

Hard Drives
Dual hard drives running RAID 1

NICs
4000
8 x 10 GigE (SFP+)

3050/3110
2 x 10 GigE (SFP+)
10 x 1 GigE (SFP)

2500
6 x 10/100/1000 (fiber GigE SX and LX available)

1200
4 x 10/100/1000 (fiber GigE SX and LX available)

Environmental
3050/3110/4000
Operating: 32° to 131°F (0° to +55°C)
Relative Humidity (Operating): 5 to 80% non-condensing

2500
Operating: 32° to 104°F (0° to 40°C)
Relative Humidity (Operating): 10 to 90% non-condensing

1200
Operating: 50° to 95°F (10° to 35°C)
Relative Humidity (Operating): 12 to 90% non-condensing

Operating System
1200/2500/3050/3110/4000
ArbOS/ArbUX, our proprietary, embedded operating systems, are based on open source operating system technology such as Linux and Open BSD.