

Stopping Denial of Service Where it Matters

Submitted by: Folliard

Wednesday, 26 May 2004

Arbor Networks Releases Peakflow SP Managed Services:

A New Revenue Source for Service Providers

Stopping Denial of Service Where it Matters

London.— May 26, 2004 – Arbor Networks®, the leading provider of network integrity solutions, today announced Peakflow® SP Managed Services, the first service provider solution for offering on-network infrastructure security services. Service providers now have a powerful new security offering for their enterprise customers, allowing them to generate revenue and build customer loyalty.

Peakflow SP Managed Services stops denial of service (DoS) attacks where it matters: in the service provider network. When a DoS attack floods an Internet uplink, the enterprise on its own is helpless. IT organisations rely on the service provider to bring its network back online. The only way to effectively block a denial of service attack is to halt the attacking traffic inside the service provider network before it reaches the enterprise customer.

Peakflow SP Managed Services makes it easy for service providers to rapidly roll out protection that encompasses the whole detection, analysis, traceback and mitigation lifecycle without requiring time-consuming network configurations. DoS protection, included in the managed services solution, is a necessity for enterprise, government and Application Service Providers that depend on the Internet for their day-to-day business. In addition, these customers are increasingly asking for greater network visibility and control, as well as detection and attack mitigation.

“Companies that depend on Internet availability can’t afford to leave themselves vulnerable to a DoS attack. Consequently, we are seeing more and more enterprises asking for enhanced security services to protect key business applications during a denial of service or other cyber attack,” said Eric Ogren, senior analyst at the Yankee Group. “Arbor Networks understands that denial of service attacks can only be addressed by service providers and are helping their service provider customers roll out these customer-facing DoS protection services.”

The Peakflow SP Managed Services module includes:

Customer-facing Portal

Peakflow SP provides a portal or “dashboard” that can be customized and that gives customers a first hand view of their traffic inside the service provider’s cloud. Using Peakflow SP, customers can log in and view reports across the lifecycle of a DoS attack. The portal also provides customers real-time traffic visualisation and access to network traffic reports.

Customer Anomaly Detection and Fingerprinting

Drawing on Peakflow SP’s rapid anomaly detection and fingerprinting capabilities, network operators now have a scalable mechanism to create an anomaly detection service. Customers can view detailed analysis of anomalous events and also determine their sources. With the ability to scale to multiple OC-192 links, Peakflow SP is the only provider-class DoS detection product on the market.

Network-wide Situational Analysis

In the face of an attack, Peakflow SP Managed Services provides network-wide analysis of the attack, a requirement for choosing the appropriate response in a complex service provider network. Customers gain a greater view into the network and consequently have a better ability to detect, mitigate and resolve an attack. The ability to determine different methods for mitigating or cleaning traffic under attack ensures that enterprises will have less data loss and better availability.

“With over 70 provider customers, we’ve gained a clear understanding of their need to offer better security and more value-added services to their customers,” said Paul Morville, director of product management at Arbor Networks. “Peakflow SP now gives service providers an easy and scalable way to offer denial of service prevention services.”

About Arbor Networks

Arbor’s network integrity systems protect organisations from zero-day security threats such as DDoS attacks and worms, and operational vulnerabilities such as inefficient peering and routing instability. Built upon the proven Peakflow platform, Arbor solutions provide accurate, real-time awareness of behavior across the entire network, enabling organizations to better secure and more efficiently operate their networks. Arbor is headquartered in Lexington, MA, with a research and development office in Ann Arbor, MI and EMEA headquarters in London. For more information, please visit <http://www.arbornetworks.com>.

Copyright (c) 1999-2004 Arbor Networks, Inc. All rights reserved. Arbor Networks and Peakflow are registered trademarks and the Arbor Networks logo and ArbOS are trademarks of Arbor Networks, Inc. in the USA and other countries. All other trademarks are the property of their respective owners.

###

For further information please contact:

Mo Murphy

Folliard,

0207 686 0625

Murphy@folliard.co.uk