

Infrastructure Security Solutions for Service Providers from Arbor Networks

■ EXECUTIVE SUMMARY

Service provider networks are increasingly vulnerable to a broad spectrum of threats – both security and operational – that can ultimately impact not just their core networks, but also customer networks. Among these threats are network worms, such as Blaster and Slammer; routing exploits; distributed denial of service (DDoS) attacks; peering instability and capacity planning issues. As they work to protect their backbone networks, providers must also meet growing customer demand for highly reliable and available network service in the midst of attacks.

For many operators, the process for responding to attacks is reactive and resource-intensive, leaving them scrambling to defend and better engineer their networks. Faced with these operational realities, leading service providers are embracing a new approach to protecting networks: modeling the normal behavior of their network as a basis for threat detection rather than attempting to model the fast-moving, chameleon-like threats that surface daily.

Arbor Networks Peakflow SP equips service providers with a network-wide, holistic view of the network. Peakflow SP does what no other security solution can do: it builds a network-wide model of the normal behavior of the network *in real-time*. Equipped with this dynamic understanding of normal network behavior, Peakflow SP instantly identifies anomalous behavior, providing actionable information that speeds resolution. Peakflow SP's anomaly detection proactively and efficiently defends the network, sidestepping the vexing false positives of signature detection.

Peakflow SP is built upon the Peakflow™ Platform, an architecture for network-wide data collection, analysis and anomaly detection. Peakflow SP is comprised of Peakflow DoS, which proactively detects and mitigates network-wide anomalies, and Peakflow Traffic, which offers insight into traffic and routing patterns across the entire network.

Together, these solutions enable service providers to bolster infrastructure security and streamline operations.

In use in many of the most demanding service provider networks in the world, Arbor's solutions are delivered on Intel Pentium® and Xeon™ processor based carrier-grade servers. Peakflow SP is the most broadly installed network anomaly detection solution in the world, with customers that include 12 leading service providers in North America and Europe, the U.S. government and several Fortune 500 companies. In addition, more than 40 evaluation deployments of Peakflow SP are underway across North America, Europe and Asia Pacific. Nearly three out of four service providers that evaluate Arbor products become customers.

■ WHERE DOES THE SOLUTION FIT?

Peakflow SP can be deployed on the backbone, at the core and at the edge of the network. Peakflow SP's scalability allows for network-wide protection based on deployment at only key routers or switches.

Peakflow SP leverages the flow data available from the routers and switches already deployed in the network. As a result, in contrast to packet-by-packet

or in-line approaches, Peakflow SP doesn't impose a performance or reliability impact upon the network; its data collection is non-intrusive. In real-time, the system compares traffic against this baseline, then flags anomalies, characterizes affected interfaces and determines the severity of the anomaly. Should an anomaly be detected, detailed anomaly information is forwarded to the Controller, which then recommends the appropriate mitigation measure to maintain service.

The platform's ability to create models of normal network behavior **from the edge through the core** – then, in real time compare traffic against these baselines to perform anomaly detection – is totally unique.



Peakflow Collectors

(Intel TSRMT2) – collect flow statistics; distill and transfer data; builds dynamic traffic baseline



Peakflow Controllers

(Intel TSRLT2) – aggregates data from collectors; create a network-wide view

■ HOW IT WORKS:

Peakflow SP's model of normal behavior provides a baseline from which anomalies can be detected as well as a basis for detailed characterization of anomaly impact by router and by interface. As such, these statistics provide the necessary foundation for accurate and actionable traceback and remediation. Peakflow SP builds its model of normal behavior across the network by analyzing flow statistics. As the de facto industry standard, NetFlow is supported by a wide range of vendors and products, including network equipment from Cisco and Juniper. In contrast to inline data collection methods, flow-based collection allows Peakflow SP to scale with your network, up to OC-192

speeds. Also, since flow comes from routers, traceback is dramatically simplified as manually mapping connections to interfaces is unnecessary – that's what routers do.

In networks where NetFlow is unavailable, Peakflow SP can generate flow statistics by examining raw packet data. Key to Peakflow SP's ability to scale across very large networks – coordinating attack detection, traceback and remediation – is its two-tier architecture of collectors, or sensing elements, and a controller, which coordinates event correlation and traceback.

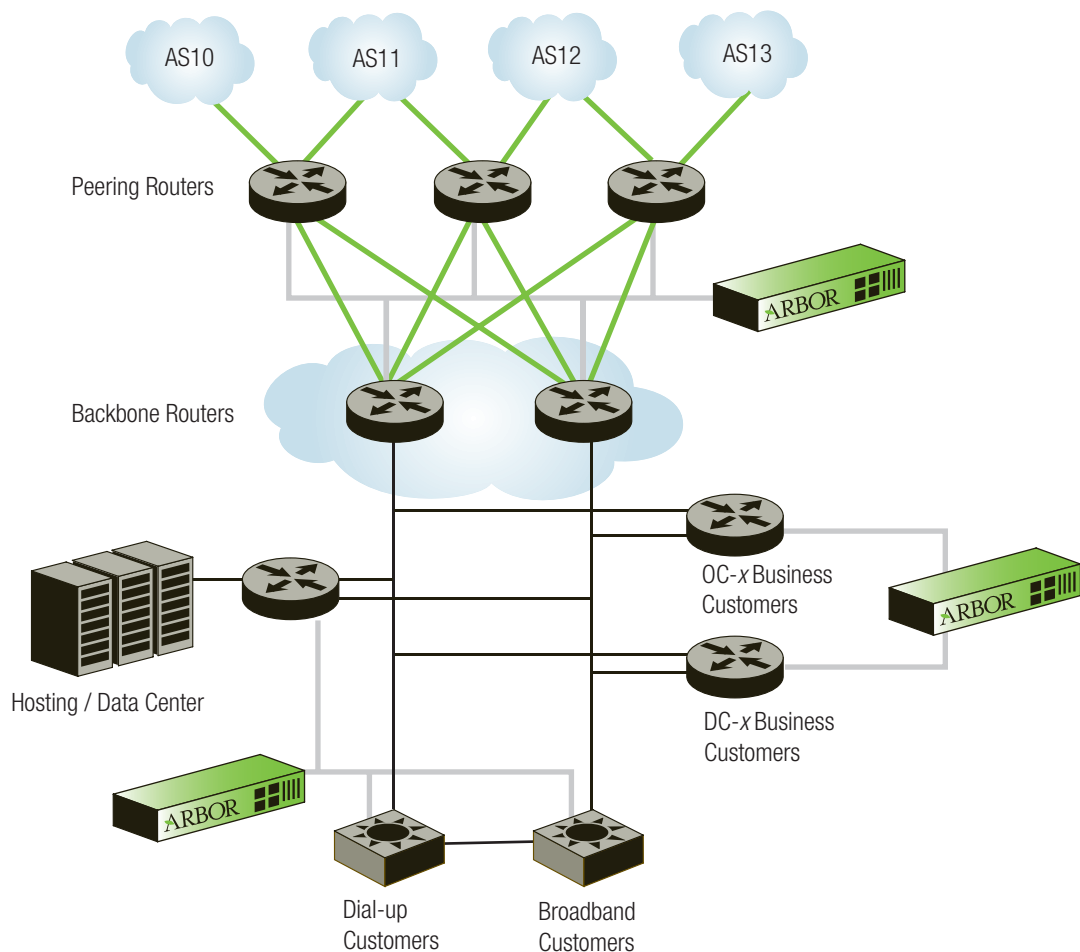


Figure 1: Peakflow SP Behavior Model

■ CARRIER CHALLENGES AND HOW THE SOLUTION ADDRESSES THEM

In addition to providing a highly reliable network day to day, service providers must meet the expectations of customers whose core business operations depend on connectivity. Customers expect to be up in the event of an attack.

In particular, Denial of Service (DoS) attacks and worms have emerged as a constant and growing concern for service providers around the world. This concern exists not just because these threats impact customers, but also because they affect service provider's core networks, and thus core business. Consider the following:

- The severity of DoS attacks continues to rise with no end in sight. Attacks with more than 10 Gbps aggregate capacity have been recorded and multi-gigabit attacks are increasingly routine.¹
 - This capacity is driven by massive pools of readily available zombies; for example, botnets with over 140,000 nodes.²
 - With so much capacity available, attackers don't even bother spoofing source addresses. Of 1,127 DoS attacks on a very large network this year, only 4 employed address spoofing.³
- The SQL Slammer worm required only 10 minutes to spread worldwide scanning over 55 million IP addresses per second. Networks at some of the largest service providers in the world were rendered unavailable as routers were overwhelmed.⁴

¹ Rob Thomas. Cisco / Team Cymru (www.cymru.com) at NANOG 28

² Ibid

³ Ibid

⁴ The Spread of the Sapphire / Slammer Worm; Moore, Paxson, Savage, Shannon, Staniford, and Weaver. (<http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html>)

These factors have several profound repercussions. First, service providers must protect their core network or risk the core data transit business and everything that rides on it. Second, service providers must offer customers meaningful protection, since more and more customers are selecting service providers based on their ability to provide this protection.

In addition to DoS attacks and worms, service providers are also faced with other areas of network-wide vulnerabilities and inefficiencies stemming from BGP misconfiguration, to misuse, or the long-term impact of changes in network utilization.

Peakflow SP provides solutions to all of these vulnerabilities by enabling service providers to:

- Compare real-time network activity against a dynamic baseline to proactively detect and resolve network-wide anomalies, including zero-day threats (e.g. attacks that spread in less than one day such as the Slammer Worm).
- Use the right fix for the right problem by utilizing black hole routing, sinkhole routing, filtering or rate-limiting remediation techniques.
- Allow tier 1 support team to resolve network threats without escalating the concern, reducing operations expense and eliminating associated SLA reimbursements.
- Export XML anomaly data to easily build analysis for forensics, trending and research.
- Easily detect, analyze and mitigate network vulnerabilities and inefficiencies, whether they stem from an attack, misconfiguration, misuse or changes in network utilization.
- Monitor traffic and topology changes across thousands of routers and interfaces from a single vantage point, providing significantly greater accuracy than manual, device-focused approaches.
- Receive immediate notification by e-mail, page or SNMP alert of anomalous activity, so the event can be promptly resolved before service suffers or customers complain.

■ SOLUTION OVERVIEW

Peakflow SP was designed for carrier-class networks. The solution is comprised of Peakflow DoS, which proactively detects and mitigates network-wide anomalies, and Peakflow Traffic, which offers insight into traffic and routing patterns across the entire network.

Peakflow DoS takes the guesswork out of attack detection, traceback and remediation. More than just automating the steps, its detailed model of normal network behavior provides the wealth of detail necessary to accurately answer questions along the way, ultimately yielding a timely and tailored mitigation result. Armed with the information they need to quickly resolve these threats, network operators can protect themselves and their customers, avoiding an otherwise reactive, time-consuming and labor-intensive process. Moreover, reliable infrastructure security helps service providers drive revenue, differentiate services, improve utilization, bolster service-level agreements (SLAs) and reduce liability for outbound attacks.

Peakflow Traffic provides a complete view of network-wide traffic and routing. Its unprecedented use of both traffic and routing data protects network infrastructure and improves backbone operations. With Peakflow Traffic, network operators can detect, analyze, and mitigate network vulnerabilities and inefficiencies, whether they stem from a routing attack, misconfiguration, misuse, or the longer-term impact of changes in network utilization.

To meet the demands of service provider networks, Peakflow SP is built on Intel's carrier-grade NEBS servers using Intel's Pentium® III and Xeon™ processors. Intel's carrier-grade servers are NEBS and ETSI-compliant which meet the stringent equipment requirements for deployment in the carrier's central office environment. Key features include:

- NEBS Level 3 and ETSI certified to withstand extreme heat, humidity, altitude and earthquake shock
- Telecom alarm panel interfaces and system management features for interfacing with central office alarm systems
- Short depth to meet central office equipment configurations
- Extended product lifecycle support to protect carrier investments

■ REFERENCE IMPLEMENTATION

Peakflow was developed to work with existing network gear, utilizing the flow from key routers in the core and at the edge. The Intel processor based carrier-grade servers (Collector and Controller) are configured for flow data (OC-192) and Packet capture (GigE) if NetFlow is not available.

Peakflow SP Technology Specifications

The complementary products, Peakflow DoS and Peakflow Traffic have different Collector and Controller specifications.

Product Specific Features:

Peakflow DoS Collectors:

- Gather NetFlow and SNMP data from routers in service provider networks to generate and maintain baselines of normal traffic patterns for the network.
- When traffic levels deviate above these baselines, the Collectors generate anomaly records and reports the relevant data to the DoS Controller.
- Each DoS Collector supports up to five routers.

Peakflow DoS Controllers

- Gather anomaly data from multiple Collectors, correlate the data and generate anomaly records.
- Provide the GUI front end for system operation and administration and generate anomaly notifications through SNMP, email and syslog.
- Each DoS Controller can manage up to 14 DoS Collectors.

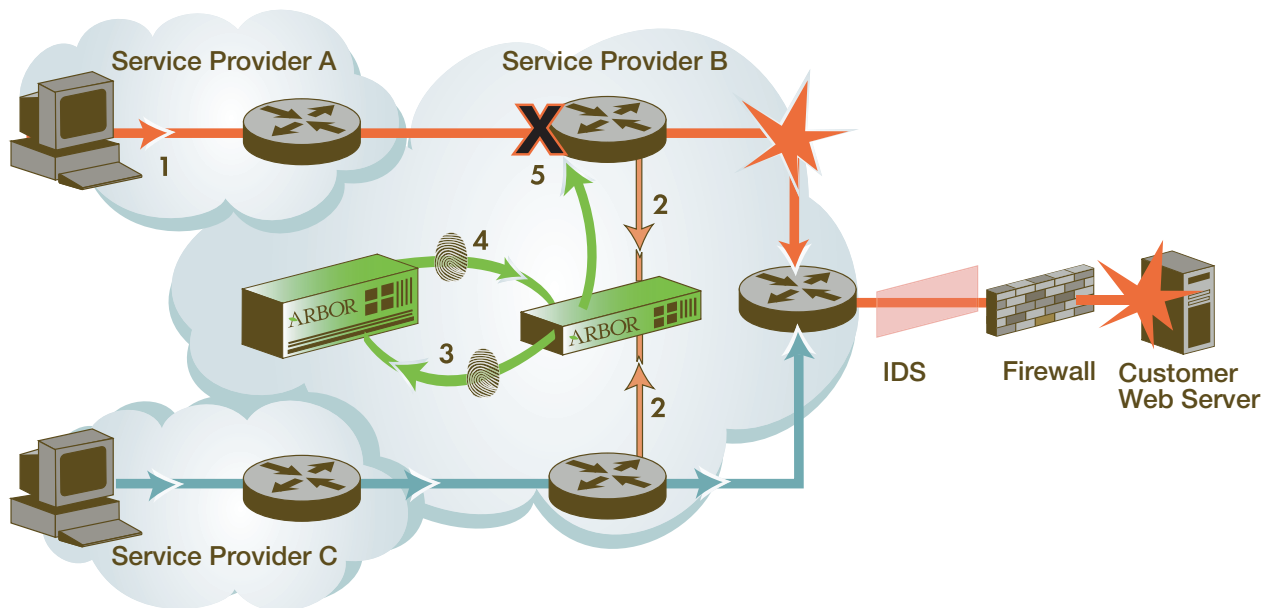


Figure 2: The diagram above shows a sample Peakflow deployment and attack example: 1) A host in Service Provider A has launched a DoS attack against a downstream customer edge router and server. 2) Service Provider B receives the attacks – however, with Peakflow continuously analyzing NetFlow statistics from key routers, it immediately detects an anomaly and 3-4) then traces the attack to Service Provider A's border, the attack source. 5) Peakflow recommends filters that the network engineer can apply to counter the attack before service is impacted.

Peakflow Traffic Collectors

- Gather NetFlow, SNMP and BGP data from routers in service provider networks and database the information for use in traffic reporting.
- Each Traffic Collector can monitor up to 8 routers.

Peakflow Traffic Controllers

- Correlate data from multiple Traffic Collectors to generate traffic and routing reports and they provide the GUI front end for users.
- Traffic Controllers have an embedded collector that can manage up to 15 routers directly.
- Support up to 9 Traffic Collectors.

Collector Hardware Specifications (both DoS and Traffic)

- The Peakflow Collector runs on Intel's dual Pentium® III processor based carrier-grade server (TRSMT2). Provides a NEBS Level 3 and ETSI certified server in a high density 1U high (1.75 inches) rack-mount form factor.
- Meet the needs of carriers wishing to deploy the collector in a hardened telco central office environment or in a back-office data center.
- The server platform is available with AC or DC power supplies for deployment flexibility.

Controller Hardware Specifications (both DoS and Traffic)

- The Peakflow Controller runs on Intel's dual Pentium® III processor carrier-grade server (TRSLT2).
- Provides a NEBS Level 3 and ETSI certified server in a high density 2U high (3.5 inches) rack-mount form factor.
- Meets the needs of carriers wishing to deploy the collector in a hardened telco central office environment or in a back-office data center.
- The server platform is available with dual AC or dual DC power supplies for deployment flexibility and high availability.
- The system comes with dual hard drives running RAID for redundancy.

OS

The Peakflow Collector and Controller run ArbOS®, Arbor's proprietary, embedded operating system, which is a hardened version of OpenBSD with all unnecessary services removed for increased security.

PERFORMANCE

Peakflow DoS supports a network consisting of up to 70 routers with a single controller. Each controller can manage up to 14 collectors that can monitor up to 5 routers each. Peakflow Traffic supports a network of up to 87 routers with a single controller. The controller can manage up to 15 routers directly and 8 collectors. Each collector can monitor up to 9 routers.

Using NetFlow, the Peakflow systems support routers with interfaces ranging from DS0 to OC-192 including newer high capacity routers like the Juniper T-640 series. Packet capture collectors support routers with interfaces up to Gigabit Ethernet speeds.

SECURITY

- Hardened OS and network stack based on OpenBSD
- Built-in firewall support, rejecting all packets by default (transparent to pings and port scans)
- All communication via SSH and SSL, using certificates issued by Arbor Networks

MANAGEMENT

- HTML access through HTTPS and command line interface access through SSH or optionally telnet
- In-band and out-of-band management available through serial console and/or management network

COMPATIBILITY

- Flow Data: Supports Cisco NetFlow v5, v7, v9; Juniper cflowd.
- Packet Capture: Supports other switches and routers using span port or third-party network tap.
- Monitoring: Integrates with management consoles supporting SNMP v1 and v2.
- Web-based UI: Internet Explorer 5.0+ and Mozilla 1.2+ using SSL.

■ TARGET MARKET AND CUSTOMER

Arbor's Peakflow SP solution is being used to help measure, visualize and protect the world's fastest and most demanding networks.

Service Providers: Peakflow SP provides customers like TELUS Corporation and Rackspace Managed Hosting, with superior network performance, rock solid security and the highest level of availability... and do so more profitably.

Cable Operators: Peakflow SP establishes tiering levels, reduces peering costs and optimizes backbone engineering while helping to grow service revenue and reducing expenses. Cox Communications has deployed Arbor's Peakflow SP to protect its network from a range of security threats.

Government: Peakflow SP streamlines infrastructure security and backbone operations, while protecting the availability of networks that carry mission-critical communications.

■ CASE STUDY / PROOF POINTS

TELUS Corporation is the largest telecommunications company in western Canada and the second largest in the country. The company provides subscribers with a full range of telecommunications products and services including data, Internet Protocol, voice and TELUS Mobility wireless services across Canada. Enterprises and providers across the country depend upon the TELUS network to be highly secure, reliable and available.

As part of TELUS commitment to adopting best-in-class technology to create a carrier class network for its customers, Arbor Networks Peakflow™ was deployed on our IP backbone in May 2002 to bolster our ability to defend the network from availability threats including distributed denial of service attacks and worms.

Peakflow™ Traffic was implemented to allow network operators to dissect TELUS' traffic for analysis both for real-time and historical reporting, providing traffic trends and other information used to properly understand the nature of traffic crossing the TELUS backbone.

Early detection of worm activity, coupled with a clear understanding of how the threat could impact the network and systems, equips TELUS to proactively defend its networks. This enables network administrators to rapidly quarantine worms, confining propagation without blocking legitimate traffic. This minimizes the service impacts and scale of infection, dramatically reducing clean-up time and expenses.

In the recent spate of worm attacks, Peakflow provided TELUS network administrators with details on exactly when the worms hit and which areas of the network were most affected, allowing them to take immediate action to mitigate the impact of the attack.

With the ever-increasing frequency, scope and diversity of attacks, including the emergence of unknown threats that cannot be predicted, it is more important than ever to approach security proactively. To reduce the impact of an attack, it is essential that service providers take advantage of the strategies available to protect against attacks that threaten network performance and ensure that threats to their traffic and their customers' service are minimized. Once an attack is underway it is essential to have the tools and expertise to track and contain it managing it to speedy and successful resolution.

From transit to hosting, TELUS customers can be confident that their services are traversing a highly available and reliable network, benefiting from the best worm defense available.

Other Peakflow SP Customer Quotes:

“Within minutes, Peakflow detected the anomalous traffic created by the worm, provided filters to mitigate the effects and pinpointed the affected servers. Our network remained available when others were still trying to figure out why their networks were saturated with traffic.”

— *Paul Fortuna, VP Engineering,
Rackspace Managed Hosting*

“Peakflow alerted us to the SQL worm well before we received the first customer call, allowing us to focus on remediating the affected servers.”

— *Tier 1 Global Service Provider*

“Given the help desk expense we would have otherwise incurred, Peakflow has already paid for itself.”

— *Tier 2 North American Service Provider*

“Arbor needs to be commended for their part in helping keep our network Slammer-free.”

— *Global Networking Solutions Provider*

■ SUMMARY

Arbor’s solutions, built on the Peakflow Platform, are deployed across the most demanding networks around the globe. Utilizing the Intel Pentium® and Xeon™ processor based carrier-grade servers, Peakflow provides network operators at leading service providers, government agencies and enterprises a solution that measures, visualizes and protects their networks. By automating threat detection, troubleshooting and mitigation, Peakflow enables the operators of these complex networks to take a proactive, holistic approach to eliminating network-wide anomalies, such as DDoS attacks, worms, router attacks, instability and policy violations. As a result, operators are able to cost-effectively tune their operations to the needs of their business, lowering operations expense while improving the security, reliability and overall performance of their network.

■ FOR MORE INFORMATION

If you would like to learn more about Peakflow please contact Arbor Networks at solutions@arbornetworks.com or call us at (toll free) 1.866.212.7267 or at +1.781.684.0900

Intel, the Intel logo, Pentium and Xeon are trademarks or registered trademarks of Intel Corporation. Copyright ©2003 Intel Corporation. All Rights Reserved.

© 2001 — 2003 Arbor Networks, Inc. All rights reserved. Arbor Networks, the Arbor Networks logo, Peakflow, and ArbOS are trademarks of Arbor Networks, Inc. in the U.S. and other countries.

