

How to Leverage Arbor Products and Services to Deliver New Managed Services

October 2007, Volume 2.0

Introduction

Arbor Networks® delivers network security and operational performance for global business networks. Arbor's Peakflow® network behavior analysis (NBA) and anomaly detection capabilities deliver unmatched network-wide visibility and scalability, enabling Internet service providers (ISPs) and global enterprises to defend against a wide range of threats, including worms, distributed denial of service (DDoS) attacks, botnets and more. Arbor Networks Peakflow solutions ("Peakflow") are deployed in more than 70 percent of the world's ISP networks, primarily for network infrastructure visibility, traffic and routing analysis, and security purposes. As a result, Arbor Networks has gained experience and established long-term relationships with the majority of the world's ISPs. Our relationships and unique experience position Arbor Networks as a key strategic partner to many ISPs. Consequently, our customers often ask us how they can leverage their existing deployment of Arbor Peakflow products to generate differentiated, next-generation services for their enterprise customers. This document, which respects customer confidentiality, contains some of the most frequently asked questions regarding managed services and our responses. For more information or a complete consultation, please contact your local Arbor Networks representative or visit our Web site at www.arbornetworks.com.

Frequently Asked Questions

What's driving the need for managed services?

Industry consolidation and plummeting bandwidth prices have made connectivity a commodity over the past five years. ISPs are desperately seeking new markets, products and services that can provide high-margin returns without substantial capital investment or the associated operational expenditures.

IP-VPN and MPLS technologies along with network services convergence are fueling the creation of these higher-margin services. Some of the more popular services associated with this convergence are Voice over Internet Protocol (VoIP), Quadruple Play, Pseudowires (PW) and Virtual Private LAN Services (VPLS). As these services emerge and their critical nature and associated requirements are inherited by IP-based protocols, new opportunities and issues present themselves to ISPs.

What Arbor product-based managed services are currently being offered?

Today, there are three main types of managed services offered by ISPs.

- **In-cloud DDoS Protection Services:** Firewall, email filtering and DDoS protection are examples of In-cloud (network-based) services. These services have arisen in response to the fact that enterprise networks can be protected from external attacks or malware much more effectively and less expensively in the clouds of ISP networks. Given the size and scale of DDoS attacks today (greater than 25Gbps), only the ISP can protect enterprises from DDoS attacks. Arbor Peakflow SP is used for this type of service.

- **IP-VPN Visibility & Security Services:** These services offer insight and reports on customer-shared or dedicated circuits. As traditional technologies such as ATM and frame relay are being replaced with IP-VPN, QoS and MPLS technologies, the need for visibility into and security of this traffic is fueling these offerings. Arbor Peakflow SP and Peakflow X products are used for this type of service.
- **Customer-Premises Managed Security:** These managed security services utilize products that are installed on customer-premises equipment (CPE) for internal network security. ISPs are beginning to roll out these CPE-based managed security services which are often integrated with SEM, content filtering and IPS/firewall solutions. Drivers for this type of security service range from compliance solutions to botnet, phishing and worm protection solutions. This type of service is gaining momentum as ISPs combine it with In-cloud services to differentiate their companies from customer premises-only managed security service providers (MSSP).

In a majority of cases today, Arbor products and services are used for In-cloud DDoS protection services—although in a recent trend, ISPs are increasingly deploying Arbor products to deliver IP-VPN visibility and security services.

Can you provide a list of ISPs who have delivered Arbor-based In-cloud DDoS protection services?

The following list represents a sample of ISPs and their In-cloud managed security services that are based upon Arbor Networks products and services.

- **Belgacom:** Clean Internet Services
www.belgacom.be/enterprises/en/jsp/static/security_processing.jsp
- **British Telecom (BT):** Managed DDoS Services
www.btplc.com/today/art69717.html
- **Cable & Wireless**
 - Anti-Distributed Denial of Service
www.cw.com/uk/services/anti-distributed_denial_of_service.html
 - Secure Internet Gateway/DDoS Protection
www.cw.com/uk/solutions/business/risk_security/story_250405_convergence.html
- **COLT:** IP Guardian
www.colt.net/uk/en/press_centre/press_releases/colt_protects_businesses_against_rise_in_computer_attacks_
- **Rackspace:** PrevenTier
www.rackspace.com/products/security/preventier.php
- **SAVVIS:** Network-Based DDoS Mitigation
www.savvis.net/corp/Products+Services/Security/Network-based+DDoS+Mitigation.htm
- **TELUS:** Managed DDoS Prevention
http://business.telus.com/en_CA/National/products/Medium_And_Large_Business/Security/Internet_And_Network_Security/details/natMlbManagedDDoS.html
- **The Planet:** Arbor Peakflow DDoS Detection
www.theplanet.com/index.html?p=arborPeakflow
- **Verizon Business:** DOS Defense Detection and Mitigation
www.verizonbusiness.com/us/security/wan/

How did these ISPs justify the creation of these services? Can Arbor share sample business cases outlining costs and ROI?

As the price of traditional services (e.g., frame relay, dedicated Internet access, private line circuits, VPN, etc.) declines due to industry consolidation, commoditization, new technologies enabling network convergence (e.g., VoIP, MPLS, etc.) and increased competition, ISPs must offer new, differentiated, revenue-generating services. In our view, since each company has its own process for the creation and approval of a business case, it is not beneficial and is a violation of confidentiality to present specific business plans here.

However, we can share the common elements of ISP business plans, including the primary drivers for offering Arbor Peakflow-based managed services. These include:

- Minimize capital expenditure by leveraging as much existing infrastructure as possible. In other words, show how Arbor Networks products can leverage flow technology in existing network infrastructure to provide visibility, capacity planning, anomaly detection and security while simultaneously being used to deliver new, differentiated, revenue-generating managed services.
- Show how time-to-market can be improved by employing “soft provisioning models.” As a result, new customers can be provisioned onto these services without “touching” the network. “Soft provisioning” means that you rely on products that utilize flow technology in your existing network infrastructure to deliver managed services that complement in-line or CPE-based products that require changes to the network.
- Deliver a positive ROI in an acceptable time frame. We have seen six-month or shorter paybacks for large projects and one- to two-year paybacks for smaller ones. In some cases, the investment is not for new service offerings but rather a vehicle to retain existing customers or expand market share. In either case, the more focus on bottom-line revenue optimization the better.
- Solve a real problem for a customer. In many business cases, the managed service has been summarized as:
 - A cost-effective means to protect enterprise networks from DDoS attacks.
 - An integral part of an enterprise’s defense in depth strategy.
 - A security, routing and traffic analysis IP-VPN solution.

To assist with justification, most business cases also contained research from well-known industry analysts. For example:

- *Next-Generation Carrier Networks Demand New Security Measures* by John S. Mazur (Gartner, April 2006) draws useful conclusions such as:
 - “Savvy NSPs will offer managed security for IP-based services to offset the challenges and expense of securing next-generation networks (NGNs) and to avoid becoming ‘commodity pipe’ providers.”
 - “A significant NSP security market will emerge as NSPs deploy overlay computing networks to oversee security.”
- *Building an ROI Methodology for Core IP Security Solutions* by Brian Partridge (Yankee Group, October 2007) makes recommendations such as:
 - “Carriers that have bet their futures on rolling out IP services will need to be more vigilant, especially against DDoS attacks, which promise to grow in both volume and complexity.”
 - “Promote your security and clean pipes. Once you have built a secure, layered architecture, tell your customers and collect a premium for their peace of mind.”

In all cases, a financial business case had to be made. Arbor Networks collaborated with Nucleus Research (www.nucleusresearch.com), a leader in ROI analysis, to create a *Peakflow ROI Tool* that can assist you in the creation of a sound, realistic business case that can ease the justification of your managed service. For more information regarding the *Peakflow ROI Tool*, please contact your local Arbor Networks representative or contact us at www.arbornetworks.com.

How much do ISPs typically charge for these services?

Arbor Networks' products and services are used mostly for In-cloud DDoS protection services, although a recent trend has seen the use of Arbor products to deliver IP-VPN visibility and security services. In most cases, the financial analysis for these services is based upon a cost and price per site. However, this could vary considerably depending on the ISP model. Therefore, the best answer to this question is "it depends." In all cases, reduction of capital expenditure is essential for the financial justification and success of the project. Arbor products lend themselves to this goal by leveraging flow technology in existing infrastructure to deliver cost-effective, pervasive visibility and security. Furthermore, Arbor Peakflow can simultaneously be utilized by network operations, network security and product management for the delivery of new profitable, non-disruptive managed services.

As mentioned previously, Arbor Peakflow products are mainly deployed today for In-cloud DDoS detection and mitigation services. In our experience, most managed DDoS services are offered and priced using one of the following two models:

1. **Subscription Pricing:** In this model, customers pay a monthly fee for accessing the service. In some cases they pay an additional per-mitigation-day fee as well. The subscription service can then be based on:
 - **Guaranteed Capacity:** The service provider guarantees that adequate scrubbing or mitigation capabilities will be in place.
 - **Best Effort:** The service provider makes its best effort to conduct mitigation, but does not guarantee that adequate scrubbing or mitigation capabilities will be in place.
2. **On-Demand Pricing:** In this model, customers pay a flat fee for each attack detection and mitigation. Customers usually seek this on-demand service when they anticipate or are in the midst of an attack. In most cases, the service will promise "best-effort" capabilities.

Beyond these pricing models, managed DDoS services can further be broken down into two main types, as described below:

- **The DDoS Detection Managed Service** is typically charged per site with an uplift on bandwidth charge. Common examples include 10 percent for a Tier 1 customer, and 15 percent for an OC3 customer, or perhaps a fixed percentage across all customers. The simple rule of thumb is the higher the speed of the link, the higher the percentage uplift for service. One large ISP is currently charging monthly rates of \$200/Tier 1 to \$70K/OC-48. However, on the other end of the spectrum, some ISPs plan to charge as little as \$1/DSL line or even eliminate the fee and make it a standard part of any Internet connection service.

We are also seeing phased deployments that target a small number of markets—such as metros, cities and regions—with the goal of attracting a specific number of new customers. Alternatively, the initial deployments are driven by customer request. In both cases, when a pre-determined goal is reached (e.g., X number of customers, or Y revenue), the ISP then expands the services to other markets and eventually network-wide or globally.

The latest trend we are seeing is ISPs delivering network-wide services—beyond the 10 to 15 percent "peering edge," closer to the "customer-edge." These services are designed to cover IP-VPN customers, broadband aggregation routers and all dedicated Internet access customers.

- **The DDoS Detection and Mitigation Managed Service** features shared and dedicated offerings that are priced according to the resources required to support the intended service. (Shared is a factor of X more affordable than dedicated, where X may represent some set of oversubscription on a mitigation device.) With mitigation, it is easier to realize ROI as long as you only have to deploy gear when you have a customer, and oversubscription is fine as long as aggregate attack rates do not exceed those of the scrubbing resources. In our experience, there are two effective deployment models for the DDoS detection and mitigation managed service, as described on the following page.

The following are the two main types of DDoS detection and mitigation:

- **Centralized or Regionalized Mitigation Centers:** In both cases, it is about getting the most ROI from capital costs. The ISP deploys some number of devices to support an intended number of shared/dedicated customers for the mitigation service. When those devices are “full,” the ISP deploys more gear to the centralized mitigation center, or to a set of regional centers in geographic areas or target markets. ISPs typically define acceptable oversubscription ratios in these models, and when the subscription ratio is reached, additional scrubbing centers or arrays of scrubbers are deployed.

In our experience, the typical ratio of customers to scrubbing devices is 6:1, while the maximum ratio tends to be 12:1. Normally ISPs do not publish these ratios as part of any service or share these capacity details with customers.

- **Customer-Specific Mitigation:** This is a less common approach in which an ISP deploys mitigation centrally (or a fan-out to specific network points) in support of a specific customer opportunity. When a new customer comes on, the ISP adds more gear.

The common rule of thumb is to follow the deployment model (centralized, regionalized or customer-specific) and make a reasonable amount of gear available to capture new customers.

Examples:

- One mitigation device per regional center.
- One dedicated mitigation device per customer. Note that dedicated in-band models are not recommended if the scale of an attack exceeds the available scrubbing capacity of a single device since service levels may be jeopardized.
- Optimizing mitigation solutions with other techniques, such as BGP black-hole routing or BGP flow specification, to allow ISPs to truly leverage distributed network-wide deployments and varying types of infrastructure capabilities. This also demonstrates the multifaceted mitigation solution array inherent in Arbor Peakflow products. For more information regarding this type of mitigation, refer to the article entitled *Deployment Experience with BGP Flow Specification* available at www.nanog.org/mtg-0610/lozano.html.

How many and what types of customers do ISPs have?

Our data indicates that ISPs range from having 25-35 customers to well over 100 customers paying for their DDoS protection services. The discrepancy in numbers is largely due to the amount of time the managed service has been on the market. In most cases, these customers are large Fortune 1000 companies. Details on exact names, number and types of customers are confidential information.

Many ISPs are targeting small and mid-sized businesses (SMB) for managed services. They see the mid-market as being virtually untapped and an area where many companies do not have in-house expertise (e.g., no CSO or security people) and thus look to their providers to support them in this capacity. ISPs are combining this service with their In-cloud services to differentiate themselves from CPE-only managed security service providers (MSSPs).

Arbor Networks has products that can be used for both In-cloud and CPE-based services. With the increased focus on network availability and the early adopters seeding the DDoS detection and mitigation market, many enterprise CIO/CISOs have budgeted for such services in 2007 and 2008.

These plans are corroborated by Arbor Networks' annual *Worldwide Infrastructure Security Report Volume III*, which was published in September 2007. The report can be downloaded from www.arbornetworks.com/report. According to the report, approximately 70 percent of the 70 service providers interviewed are currently delivering or plan to deliver some sort of DDoS protection service. This was mainly due to customer demand for such services.

When do ISPs typically stop the mitigation?

Unfortunately, the answer to this question is “it depends.” Active mitigations can run from minutes to months, depending on the type of attack and the amount of scrubbing resources. Some customers are in permanent scrubbing scenarios and require dedicated scrubbers to handle Off-ramped traffic and provide ongoing protection.

Do you have any insight into the types of SLAs that are being offered for managed services?

At this time, service level agreements (SLAs) based upon In-cloud DDoS detection and protection services seem a little premature. In general, most SLAs are based on “time to response”, rather than a guarantee of attack detection or mitigation. In other words, we do not see any SLAs guaranteeing “a 99 percent clean pipe” or “stopping an attack in 15 minutes.” Instead, most SLAs guarantee response and engagement time frames. These response times are typically 15-20 minutes after attack detection or notification by the customer.

The following link contains an example of such an SLA from Verizon Business www.verizonbusiness.com/terms/us/products/security/dosdefense/.

Which Arbor products and services are being deployed for the managed services outlined above?

There are three types of managed services that are based upon Arbor Networks products. The following is an outline of the Arbor products (at a very high level) used to deliver each of these managed services. For more information regarding Arbor products and/or assistance with a detailed design for your managed service, contact your local Arbor Networks sales representative or visit our Web site at www.arbornetworks.com.

Arbor Managed Services

IN-CLOUD MANAGED SECURITY SERVICES: DDOS DETECTION & MITIGATION

Product(s)

- Arbor Peakflow SP Collector Platform (CP) devices
- Arbor Peakflow SP Flow Sensor (FS) devices
- Arbor Peakflow SP Business Intelligence (BI) devices
- Arbor Peakflow SP Threat Management System (TMS) devices
- Arbor Peakflow SP Managed Services (MS) licenses

Description

Arbor Peakflow SP CP, FS and BI devices leverage flow information in existing network infrastructure equipment to provide cost-effective visibility into VPN/MPLS networks. These products can also detect and help mitigate DDoS attacks.

- Arbor Peakflow SP TMS is a device specifically designed to mitigate a DDoS attack by surgically removing the attack traffic while keeping the legitimate business traffic. There are three models of Peakflow SP TMS devices that allow you to optimize your deployment and services: Peakflow SP TMS 1200 (small), Peakflow SP TMS 2200 (medium) and Peakflow SP TMS 2700 (large).
- Arbor Peakflow MS licenses allow the products mentioned above to be used for managed services.

IP-VPN VISIBILITY AND SECURITY SERVICES

Product(s)

- Arbor Peakflow SP Collector Platform (CP) devices
- Arbor Peakflow SP Flow Sensor (FS) devices
- Arbor Peakflow SP Managed Services (MS) licenses
- Arbor Peakflow X devices

Description

Arbor Peakflow SP (CP, FS) and Arbor Peakflow X devices leverage flow information in existing network infrastructure equipment to provide cost-effective visibility into VPN/MPLS networks. These products can provide information such as top talkers, conversations and applications per VLAN ID, ASN, customer, MPLS labels, QoS bit or router interfaces. Arbor Peakflow X secures the IP-VPN by detecting internal network threats such as zero-day worms, phishing, pharming and inside misuse that traditional perimeter/signature-based security products cannot detect.

- Arbor Peakflow MS licenses allow the products mentioned above to be used for managed services.

CUSTOMER-PREMISES MANAGED SECURITY

Product(s)

- Arbor Peakflow X devices

Description

Traditional customer premises-based security services involve security products such as firewalls, IDS/IPS or anti-virus. Arbor Peakflow X complements these products by leveraging flow technology in switches and routers to deliver cost-effective, pervasive visibility for both operational and security purposes. Arbor Peakflow X detects internal network threats such as zero-day worms, phishing, pharming and inside misuse that traditional perimeter/signature-based security products cannot detect.

- Arbor's Security Engineering and Research Team (ASERT) is a team of security experts who monitor global threat activity and distribute network behavioral fingerprints via the Active Threat Feed (ATF) service to Arbor Peakflow customers to help them stay abreast of the most critical threats to their network.

How will Arbor Networks help me?

Arbor Networks offers a wealth of experience and expertise when consulting with ISPs on how to leverage their existing investment in Arbor products to generate new managed services. Arbor Networks also has the unique ability to bridge across many silos within an ISP's organization (e.g., infrastructure security, operations, MPLS and IP-VPN, SLA compliance, reporting per product, specialized visibility teams, etc.) and create capital efficiencies that can drive new high-margin revenue—both bottom line and top line—within their specific product sets.

Below are some common ways ISPs utilize Arbor Networks to help launch managed services:

- Help conduct financial analysis that will be required to justify the investment in the managed service. Arbor Networks has multiple financial analysis tools such as the *Peakflow ROI Tool* that you can leverage.
- Help expose and provide ways to overcome potential roadblocks to the complex, multi-department justification process, product launch and support of the managed service.
- Help determine the ISP's strengths and differentiators that can be leveraged for a unique managed service.
- Provide technical design for Arbor products that will serve as the foundation for the managed service.
- Provide operations, sales and marketing training, support and go-to-market assistance.
- Assist with Arbor product deployment, custom integration and packaging within their operating environment.



Corporate Headquarters

430 Bedford Street
Lexington, Massachusetts 02420

Toll Free +1 866 212 7267
T +1 781 684 0900
F +1 781 768 3299

Europe

T +44 208 622 3108

Asia Pacific

T +86 10 8529 8885

www.arbornetworks.com

Copyright ©1999-2007 Arbor Networks, Inc.
All rights reserved. Arbor Networks, the
Arbor Networks logo and Peakflow are
all trademarks of Arbor Networks, Inc.
All other brands may be the trademarks
of their respective owners.

FAQ/US/1007

In many cases, the managed service is deployed in a phased manner. Arbor Networks has unique talents and products to assist with each phase. In fact, the Arbor products are built for phased, success-driven deployments where the goal is to first deliver successful customer penetration before a second deployment cycle is approved. This model has been proven and is in use today with several customers employing an array of different models (e.g., shared service, customer specific, etc.).

In some cases, Arbor Networks' personnel have acted as a representative of the ISP's organization. In these cases, Arbor's staff has participated in sales calls, seminars and other marketing-related activities. Understandably, we have found that the best approach is to focus Arbor Networks' efforts on making sure the ISP is as self-sufficient as possible.

The bottom line is that Arbor Networks is committed to your success in launching, scaling and reducing the risks associated with new In-cloud or CPE-based managed service offerings. For more information about how your organization can use Arbor Networks products and services to help launch managed services, please contact your local Arbor Networks representative or visit us at www.arbornetworks.com.

About Arbor Networks

Arbor Networks provides network security and operational performance for the world's global business networks—protecting networks from the service provider cloud to the enterprise core. Arbor Peakflow products deliver network-wide visibility, anomaly detection and scalability to defend against current and future threats, including worms, data theft, botnets and more. Arbor Peakflow enables businesses to harden their networks, maintain business continuity and prevent the loss of customer confidence. Arbor is headquartered in Lexington, MA, with a research and development office in Ann Arbor, MI, and overseas headquarters in London and Beijing.