FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

Arbor Networks Enables DDoS Protection for Hosting and Cloud Service Providers

Securing the Data Center and Generating Revenue

A Frost & Sullivan
White Paper

Richard Martinez
Research Analyst

www.frost.com

CONTENTS

INTRODUCTION

The single biggest factor holding back enterprises from leveraging hosting and cloud service providers continues to be security and availability concerns. There is an inherent loss of control when moving corporate data and applications into the "Cloud". For many organizations, it is a leap of faith that they are simply not ready to make. For hosting and cloud service providers, this presents both a challenge and a revenue-generating opportunity.

Concerns over security and availability are not without merit. Daily, one can read media headlines of another Distributed Denial of Service (DDoS) attack victim. The threat of DDoS attacks is especially insidious in the hosted and "cloud" environments. Due to the multi-tenant nature of these environments, DDoS attacks can have a cascading impact on, not only the targeted customer, but others within the shared infrastructure, not to mention the impact on the service providers themselves.

The impact is the same for both customer and service provider - downtime, which means lost revenue; unhappy customers, which causes customer churn; operational costs associated with mitigating the attack; marketing costs to retain and attract new customers and perhaps most important, damage to the brand and reputation.

There's little doubt that as the size, frequency and complexity of DDoS attacks continue to rise, hosting and cloud service providers must have solutions in place to protect the availability of their infrastructure and services. In fact, as enterprises become more educated about the frequency and impact of DDoS attacks, they will demand such protection from their hosting or cloud service provider-before they move their business to the "cloud". Surprisingly, today not many hosting or cloud service providers offer the proper protection from modern day DDoS attacks. Therefore, hosting and cloud service providers that can demonstrate such comprehensive DDoS attack protection stand to benefit from competitive differentiation and increased revenue derived from managed DDoSattack protection services.

This paper will provide an overview of the latest DDoS attack trends, give examples of how hosting and cloud service providers can use the Arbor Networks products and services to protect the availability of their data center infrastructure and services from DDoS attacks and increase revenue by offering Arbor-based, managed DDoSattack protection services.

DDOS ATTACK TRENDS

DDoS attacks have been around for a number of years. What has changed, however, are the size, frequency and complexity of these attacks. There are several reasons behind this disturbing trend. Two of the primary reasons are:

1. **Motivation –** In the past, the most common motivation behind DDoS attacks was individual financial gain (i.e. extortion) or notoriety. Many of today's DDoS attacks are politically motivated. For example, a whole new breed of attacker, known as "hacktivists", has emerged to launch DDoS attacks against organizations simply because they -disagree with their political or social stances. (e.g. Anonymous attacks on financial organizations). There are also many state-sponsored organizations that are behind DDoS attacks, creating the new threat of cyber warfare.
2. **Ease of Attack –** DDoS attacks are no longer conducted by tech-savvy experts. Today, there is a plethora of - DDoS attack tools (e.g. LOIC, SOIC) or botnets for hire readily available to the common Internet user. Combine the capability to quickly organize a group of hacktivists with the use of social media (e.g. Facebook, Twitter etc.) and one can see how easy it is to launch a DDoS attack.

There are three main categories of DDoS attack:

Volumetric Attacks: These attacks attempt to consume the bandwidth either within the target network/service, or between the target network / service and the rest of the Internet. These attacks are simply about causing congestion. Volumetric attacks are not new and first emergingin 2001. Well publicized examples were when Microsoft, eBay and Yahoo! were taken offline. Back then, these DDoS attacks – in the 300Mbps range - were considered "large" volumetric attacks. Today, DDoS attacks routinely exceed 100Gbps.

TCP State-Exhaustion Attacks: These attacks attempt to consume the connection state tables which are present in many infrastructure components such as load-balancers, firewalls and the application servers themselves. Even high capacity devices capable of maintaining state on millions of connections can be taken down by these attacks. In fact, Frost & Sullivan has observed,

"A common response by many administrators to the challenges of DDoS is the belief that their firewall and IPS infrastructure will protect them from attack. Unfortunately, this is not true. Firewalls and IPS devices, while critical to network protection, are not adequate to protect against complex DDoS attacks."

Application-Layer Attacks: In 2010, there was a dramatic shift in DDoS attacks from primarily large volumetric attacks to smaller, harder-to-detect, application-layer attacks that target some aspect of an application or service at Layer-7. These more stealth attacks can be very effective with as few as one attacking machine generating a low traffic rate (this makes these attacks very difficult to proactively detect and mitigate).

As one can see, DDoS attacks have evolved from relatively simple brute force bandwidth consuming attacks, conducted by a limited set of individuals, to a combination of very large and stealth attacks capable of being executed by just about anyone. This paper will examine the key issues that DDoS attacks present to hosting and cloud service providers and how Arbor Networks solutions can be utilized to address these challenges.

PROTECTING THE AVAILABILITY OF DATA CENTER INFRASTRUCTURE & SERVICES

Until fairly recently, the occurrence of DDoS attacks under 10 Gbps were few and far between. According to the Arbor Networks Worldwide Infrastructure Security Report[1], over the course of 2010-2011, the market witnessed attacks reaching 60-100 Gbps, and they are only expected to continue to increase in scale. While these volumetric attacks can wreak havoc for data center operators, application-layer attacks can be even more threatening to services running within data centers. Because firewalls, IPS, and load-balancer devices are susceptible to state exhaustion attacks, data center operators must implement the appropriate solutions to withstand and mitigate these attacks against their network infrastructure. Furthermore, DDoS attacks are becoming increasingly sophisticated through the combined use of volumetric and application-layer attacks. The bottom line is modern day DDoS attacks pose a substantial threat to data center availability.

This is occurring at a time when security concerns about cloud computing continue to be top of mind for IT executives. In fact, according to a May, 2012 Stratecast report titled, ***Cloud's Security Risk Premium: Poised to Drop?***

"Despite the maturing of cloud services, and the constant marketing of cloud benefits, the original concern of security within the cloud remains unabated. In the three years that Stratecast has been surveying IT decision makers, their perceptions on security risk associated with cloud computing has remained essentially unchanged, at least relative to the risk they associate with their on-premises private data centers."

In an environment where high availability of services and applications are key requirements within today's data centers[2], any type of downtime can not only negatively affect revenues, but also customer perception.

In a survey[3] of IT professionals conducted by Neustar, nearly two-thirds of respondents indicated that a DDoS attack would cost $240,000 in revenue losses per day. The same report showed that over 50 percent of respondents were concerned about the potential damage to their customer experience. Due to the multi-tenant and shared environment in today's modern data center, a DDoS attack can cause broad collateral damage, ultimately resulting in a one-to-many attack - of significant appeal to attackers.[4]

[1] Worldwide Infrastructure Security Report, 2011 Volume VII

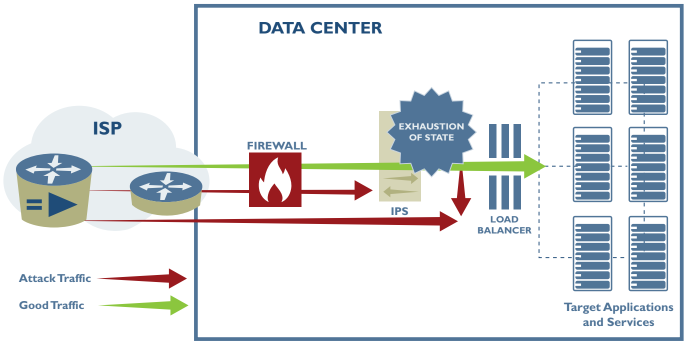
[2] Depulsio's DDoS Protection Service powered by Arbor Networks solutions: Peakflow SP and Peakflow SP TMS, Pravail APS and Cloud Signaling

[3] http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240000446/what-a-ddos-can-cost.html

[4] http://www.datacenterknowledge.com/archives/2011/10/11/mitigating-intelligent-ddos-attacks/

With a potential loss of revenue, and gain of negative customer perception resulting from a DDoS attack, hosting providers and data center operators must be able to demonstrate to their customers that they are implementing the technology necessary to combat these threats. Traditional network security devices, such as firewalls and IPS, no longer meet minimum protection requirements, and can themselves become targets of a DDoS attack – a frustrating situation, indeed, when an outage is caused by a mitigation system.

Figure 1 - Firewalls and IPS are vulnerable to DDoS Attacks



Source: Arbor Networks

More specifically, since firewalls and IPS are stateful devices, they must maintain the state of each conversation that traverses through them. Attackers know this and routinely exploit this vulnerability by launching connection-layer attacks (i.e. TCP SYN flood) which are designed to fill state tables in firewalls and IPS, ultimately causing these inline solutions to fail and potentially stop all traffic traversing through them,-thus completing the DDoS attack for the attacker. Additionally, most DDoS attacks utilize legitimate HTTP (TCP port 80) or HTTPS (TCP port 443) traffic. By default, this traffic is "allowed" by firewalls and IPS. In other words, the attack traffic simply flows through what is, many times, the only line of defense for the data center.

So what is the solution to stopping today's modern-day DDoS attacks? **Intelligent DDoS Mitigation Systems (IDMS).** These solutions were designed from the ground up to detect and stop DDoS attacks. Some of the key characteristics of an IDMS are:

- Support both -inline and, more importantly, out-of-band deployment to avoid being a single point of failure on the network.
- True "distributed" DoS (DDoS) attack detection, which requires broad visibility into the network (not just from a single network perspective) and the ability to analyze traffic from different parts of the network.
- Attack detection using multiple techniques, such as statistical anomaly detection, customizable threshold alerts and fingerprints of known or emerging threats that are based on Internet-wide intelligence.
- Mitigation that can easily scale to handle attacks of all sizes, ranging from low-end (e.g., 1Gbps) to high end (e.g., 40Gbps).

Arbor Networks offers such an IDMS for comprehensive DDoS Protection in the data center.

ARBOR NETWORKS' COMPREHENSIVE DDOS SOLUTIONS

Arbor Networks offers two different solutions for comprehensive DDoS protection:

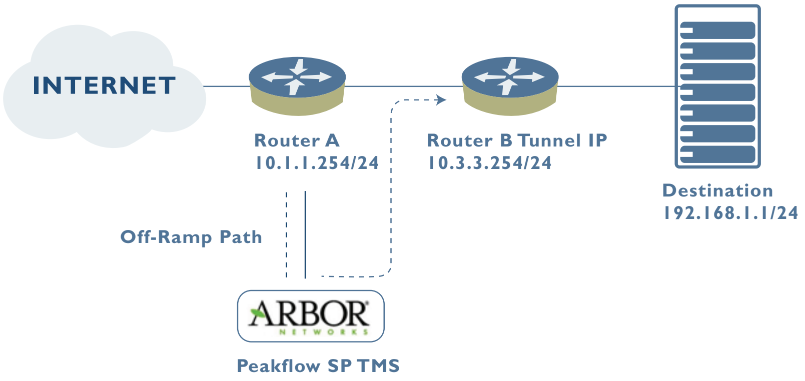
1. **Peakflow –** designed for the larger, more complex data center
2. **Pravail –** designed for the smaller, less complex data center

The hosting or cloud service provider's network environment and security team's capabilities determine which solution - is right for them. The following is a description of the two Arbor solutions.

ARBOR'S PEAKFLOW SOLUTION

Arbor's Peakflow solution is designed for the more complex and larger data center environments. More specifically, data centers that have Internet circuits larger than 10 Gbps, support IPv4 and IPv6 traffic and utilize the BGP routing protocol. There are two major components to the Peakflow solution. The first is **Peakflow SP.** Peakflow SP leverages IP flow (e.g. Netflow) and routing information embedded in the existing data center network infrastructure to deliver cost-effective network visibility. Peakflow SP automatically conducts network anomaly detection and subsequently can easily detect threats, such asDDoS attacks. Upon DDoS attack detection, Peakflow SP alerts network and security operations staff; that then mitigate the attack using the second component of the Peakflow solution- **Peakflow SP Threat Management System (Peakflow SP TMS).** It's important to note that the Peakflow SP TMS appliance is not an inline device. Using the BGP routing protocol, both attack and legitimate traffic is routed to the Peakflow SP TMS device where only the attack traffic is surgically removed. The legitimate traffic is then re-injected back into the network using a tunneling protocol (e.g. GRE) where it continues onto its original destination.

Figure 2 - Out-of-Band Mitigation with Arbor Peakflow SP TMS



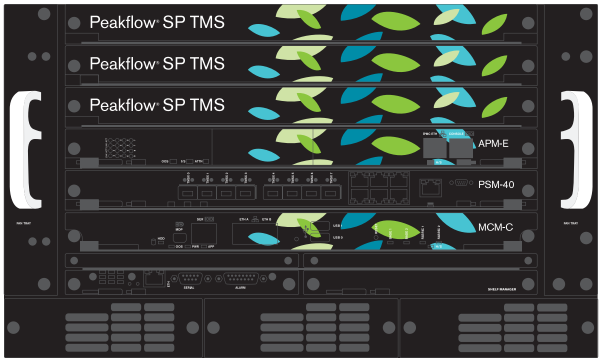
Source: Arbor Networks

One of the main advantages of deploying Arbor Peakflow SP TMS out-of-band, as shown in Figure 2, is the ability to create a virtual local area network (VLAN) and deploy the appliance outside the core network. This ensures that, if for some reason, the Peakflow SP TMS appliance encounters problems,it will not be the point of failure for a network outage. Hosting providers SdVPlurimedia and Hostopia credit the ability to send a mix of legitimate and attack traffic "out of band" to the Peakflow SP TMS for mitigation as a major factor in selecting an Arbor Networks-solution5.[5]

Peakflow SP TMS comes in a variety of models that allow the mitigation of attacks ranging from 1 Gbps to 40 Gbps.

The Peakflow SP TMS has counter measures - that can be used to stop a number of networks and application-layer DDoS attacks, some of which are listed below.

Figure 3 - Peakflow SP TMS 4000



Source: Arbor Networks

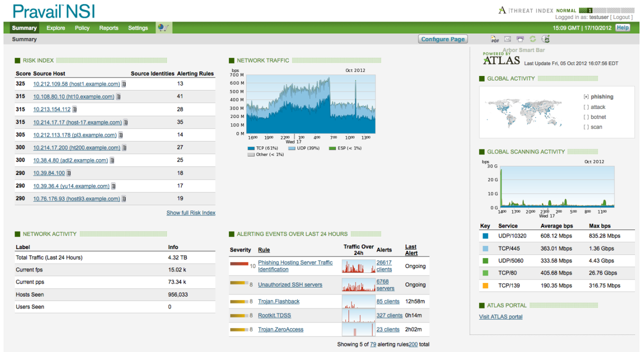
- Flood Attacks (TCP, UDP, ICMP, DNS Amplification)
- Fragmentation Attacks (Teardrop, Targa3, Jolt2, Nestea)
- TCP Stack Attacks (SYN, FIN, RST, SYN ACK, URG-PSH, TCP Flags)
- Application Attacks (HTTP GET floods, SIP Invite floods, DNS attacks, HTTPS protocol attacks)

[5] http://www.crn.com/blogs-op-ed/channel-voices/240002568/how-to-prevent-ddos-attacks.htm

ARBOR'S PRAVAIL SOLUTION

Arbor's Pravail solution consists of two major components: **1) Pravail Network Security Intelligence (NSI)** and **2) Pravail Availability Protection Solution (APS)**. The Pravail solution has been designed to be deployed within smaller, less complex data center environments. For example, data centers that have 10Gbps or less of Internet connectivity or are staffed with less experienced security operations personnel.

Figure 4 - Detection of Botnet Traffic with Arbor Pravail NSI



Last Update Fri, 05 Oct 2012 16:07:56 EDT

RISK INDEX

Score	Source Host	Source Identities	Alerting Rules
325	10.212.109.58 (host1.example.com)		13
315	10.108.80.10 (ht10.example.com)		41
315	10.213.154.112		28
315	10.214.17.17 (host-17.example.com)		35
305	10.212.113.178 (pl3.example.com)		14
300	10.214.17.200 (ht200.example.com)		27
300	10.38.4.80 (adl2.example.com)		25
290	10.39.84.100		18
290	10.39.36.4 (yu14.example.com)		17
290	10.76.176.93 (host93.example.com)		19

Show full Risk Index

NETWORK ACTIVITY

Label	Info
Total Traffic (Last 24 Hours)	4.32 TB
Current fps	15.02 k
Current pps	73.34 k
Hosts Seen	956,033
Users Seen	0

ALERTING EVENTS OVER LAST 24 HOURS

Severity	Rule	Traffic Over 24h	Alerts	Last Alert
10	Phishing Hosting Server Traffic Identification		26617 clients	Ongoing
8	Unauthorized SSH servers		6768 servers	Ongoing
8	Trojan.Flashback		85 clients	12h58m
8	Rootkit.TDSS		327 clients	0h14m
8	Trojan.ZeroAccess		23 clients	2h02m

Showing 5 of 79 alerting rules200 total

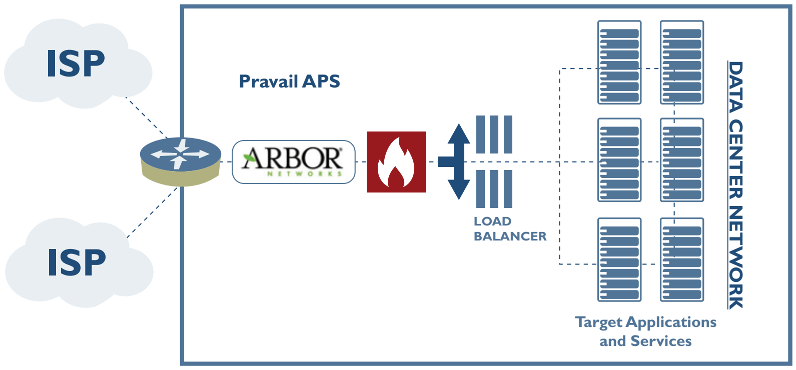
Key	Service	Average bps	Max bps
🟦	UDP/10320	608.12 Mbps	835.28 Mbps
🟦	TCP/445	363.01 Mbps	1.36 Gbps
🟩	UDP/5060	333.58 Mbps	4.43 Gbps
🟩	TCP/80	405.68 Mbps	26.76 Gbps
🟧	TCP/139	190.35 Mbps	316.75 Mbps

Source: Arbor Networks

Pravail NSI leverages IP flow technology (e.g. NetFlow) embedded in routers and switches within the data center. Pravail NSI gathers and analyzes IP flow information to provide visibility into data center traffic and uncover misuse, malicious behavior and other activity that could cause harm to the network or customer services. Using Deep Packet Inspection (DPI) technology, the **Pravail NSI Application Intelligence Collector** extends the visibility of Pravail NSI up to the application layer, providing a single, integrated solution for detecting and thwarting advanced attacks that can lead to fraud or leakage of confidential or proprietary information.

To stop both network and application-layer DDoS attacks in data centers, Arbor offers **PravailAPS**. Pravail APS is based upon the same proven carrier- grade, technology as in the Peakflow SP Threat Management System. The **Stateless Analysis Filtering Engine (SAFE)** is a uniquepacket-based engine that provides the foundation for Pravail APS. Unlike load balancers, IPS or firewalls, SAFE detects and mitigates most DDoS attacks without tracking any session state. In cases where tracking is required, SAFE only stores minimal information for a short period of time. As a result, Pravail APS can withstand the low-volumetric attacks that hinder other products and threaten availability. In fact, in many cases, Pravail APS is deployed in front of firewalls or IPS to protect them from DDoS attacks.

Figure 5 - Arbor Pravail APS deployed in front of firewalls and IPS



Source: Arbor Networks

The Pravail APS appliance comes in a variety of models, providing 1Gbps to 10Gbps of attack mitigation capacity.

PRODUCTS BACKED BY INDUSTRY EXPERTISE

The Arbor Security Engineering Research Team (ASERT) is a recognized leader in global threat research and protection. Both the Peakflow and Pravail product lines are backed by ASERT's expertise. The results of ASERT's analysesare transformed into feeds that automatically update the Peakflow and Pravail products. For example, the Active Threat Feed (ATF) and ATLAS Intelligence Feed (AIF) arm - Peakflow and Pravail products with up-to-date security intelligence enabling hosting and cloud service providers to detect and correlate network activity that would indicate a security risk, such as bots or malware.

GENERATE REVENUE WITH MANAGED DDOS PROTECTION SERVICES

It is well known that before enterprises will consider migrating their businesses to "the cloud", they must be convinced that their hosting or cloud service provider has adequate DDoS protection in place. Therefore,it is in the best interest of the service provider to highlight its DDoS attack protection capabilities, as-these services can be - competitive differentiators and sources of new revenue. Arbor Networks Peakflow and Pravail products can be used to deliver such services. With features such as APIs, mitigation templates, alerting and reporting and customer portals, the Arbor products offer a platform to deliver managed DDoS attack protection services. In fact, today there are many large and small hosting and cloud service providers who sell managed DDoS protections services based upon Arbor products and services. Below are -quotations from a few of these Arbor customers:

"We chose Arbor's Peakflow SP and TMS solutions because of their ability to deliver a holistic, out-of-band solution that can not only detect, but also defend against DDoS attacks." — Dirk Bhagat, chief technology officer, Hostopia

"It's not a matter of choice, it's a matter of survival… If we didn't have a working Arbor DDoS protection solution in place, all our customers would leave and we would be out of business." — Salim Gasmi, chief technology officer, SdV Plurimedia

"To show our customers that we are serious about service, we highlight the use of industry-leading products such as Arbor Peakflow SP as proof that we are investing in our data center infrastructure. We see this as a win-win for Arbor and iWeb." — Olivier Legault, marketing director, iWeb Technologies

FINAL WORD

DDoS protection should not be treated as a 'one-size fits all' solution. Understanding the types of DDoS attacks, and their different targets, will enable hosting and cloud service providers to choose appropriate solutions. As DDoS attacks continue to grow in magnitude and sophistication, it is essential for hosting and cloud service providers to equip their data centers and cloud environments with the solutions necessary to effectively mitigate these attacks. Understanding that a DDoS attack can result in severe financial and reputation loss, the need for purpose-built solutions is critical. Arbor Networks' DDoS solutions provide hosting and cloud service providers with a range of flexible and reputable solutions to effectively protect the availability of their data centers and generate revenue from managed DDoS attack protection services.

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost • myfrost@frost.com
http://www.frost.com

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Detroit
Dhaka
Dubai
Frankfurt
Hong Kong
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Mexico City
Miami
Milan
Mumbai
Moscow
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC