

Layered Intelligent DDoS Mitigation Systems

WHY INTERNET SERVICE PROVIDERS ARE IN A UNIQUE POSITION TO DELIVER LAYERED DDoS ATTACK PROTECTION SERVICES

Executive Summary

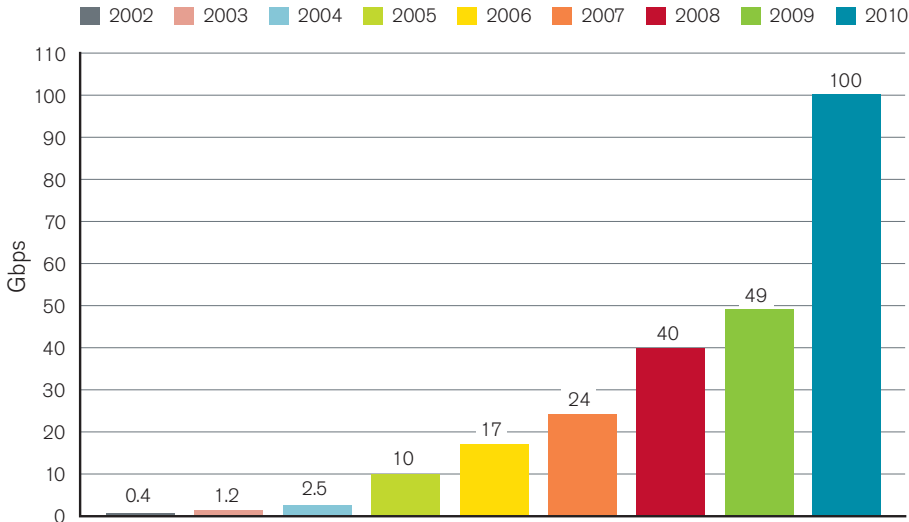
Whether you're an ISP, a hosting company, a data center operator offering "cloud services," or all of the above, you are no doubt facing multiple business challenges. Increasing competition; corporate pressure to expand market share, ARPU and profitability; shrinking staff size; and reduced CAPEX/OPEX budgets. Today's business environment is clearly tougher than ever.

Given these challenges, how do you retain existing customers—and attract new ones? One approach is to offer customers more high-valued services, such as managed security. As the size, frequency and complexity of DDoS attacks increase, security and availability are your customers' top requirements. To make matters worse, traditional security products such as firewalls or intrusion prevention systems are inadequate when it comes to stopping today's volumetric and application-layer DDoS attacks.

The solution? A layered Intelligent DDoS Mitigation System (IDMS). This paper examines some of the latest DDoS attack trends and provides some best practices when it comes to delivering a layered DDoS protection service that can help maintain availability and security. It also highlights how the Arbor Peakflow® SP solution ("Peakflow SP"), Arbor Peakflow Threat Management System ("TMS") and Pravail™ Availability Protection System ("APS") can provide a comprehensive and layered IDMS solution that extends from the data center to the ISP cloud.

The Growing and Evolving DDoS Threat

Over the last two years, the term "DDoS attack" has made its way into the public media stream. Today even non-technical people are aware of the existence and potential impact of such attacks. In years past, DDoS attacks have been dominated by "volumetric" attacks usually generated by compromised PCs that are grouped together in large-scale botnets. Some well-publicized examples include the DDoS attacks against UK-based online betting sites¹ where the hackers extorted the gambling firms, and the politically motivated DDoS attacks against the Georgian government.² This type of DDoS attack is generally high bandwidth and originates from a large number of geographically distributed bots. The size of these volumetric DDoS attacks continues to increase year over year, and they remain a major threat to enterprises and ISPs alike. In fact, according to Arbor's sixth annual *Worldwide Infrastructure Security Report* (2010), the largest reported DDoS attack was 100 Gbps—representing a 100% increase over the size of attacks reported the prior year.



DDoS attack size over time
Source: Arbor Networks, Inc.

¹ news.bbc.co.uk/2/hi/technology/4169223.stm

² www.cnn.com/2009/TECH/08/07/russia.georgia.twitter.attack

Not only are attacks increasing in size, but they are also increasing in complexity as new types of DDoS attacks continue to emerge and threaten the availability of Internet-facing businesses and services. Conduct a quick search on the Internet and it's not difficult to find media coverage regarding online banking, e-commerce and even social media sites that have been victims of application-layer DDoS attacks.

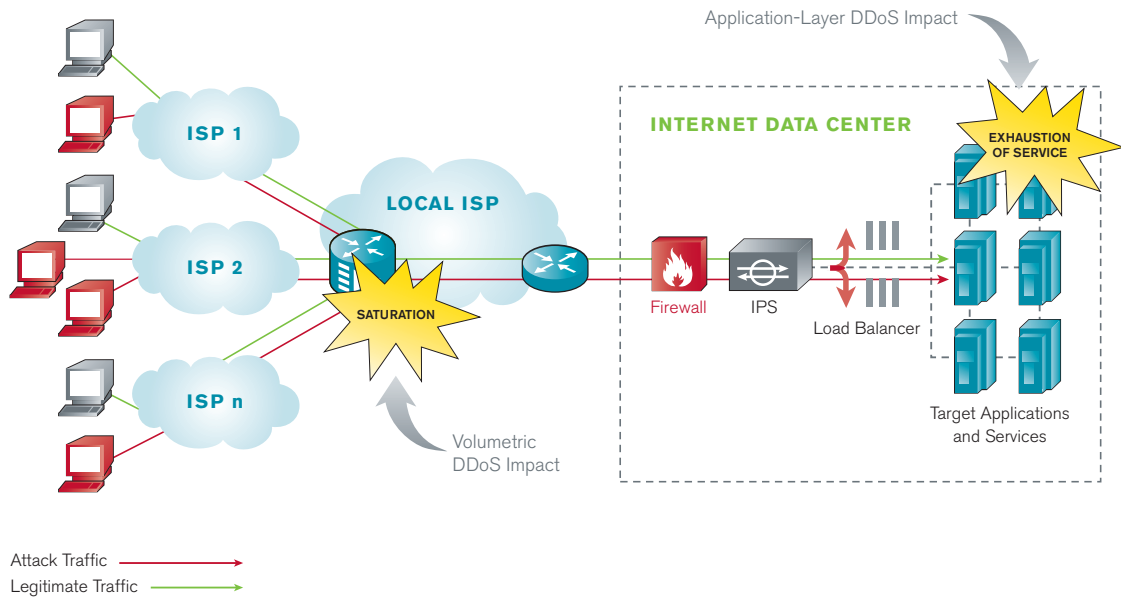
The motivation? Most of the time it's for financial gain, but other incentives include political "hactivism" or just plain old ego. And thanks to a growing trend of do-it-yourself attack tools and "botnets for hire," even a computer novice can execute a successful DDoS attack. For example, possibly one of the most publicized series of DDoS attacks happened in 2010 when a group of Wikileaks supporters and hactivists known as "Anonymous" used social media sites to recruit and instruct supporters on how to download, configure and execute an application-layer DoS attack against several targets (the group called these attacks "Operation Payback"). For those supporters who were not computer-savvy enough to conduct the DDoS attacks themselves, there was an option to "Volunteer your PC for the Cause," in which case a member of Anonymous would take over the supporter's PC and make it part of the botnet!

The bottom line: Never before has it been easier to execute a DDoS attack.

Two Classes of DDoS Attacks

Though there are many attack vectors, DDoS attacks can be categorized into two main classes:

1. **Volumetric Attacks:** These are "flooding" type attacks that are designed to saturate and consume network bandwidth and infrastructure. Examples include ICMP, UDP or TCP SYN floods.
2. **Application-Layer Attacks:** These attacks use much less bandwidth than volumetric attacks. They are therefore harder to detect and designed to target specific applications/services where they slowly exhaust resources. Examples include HTTP or DNS attacks.



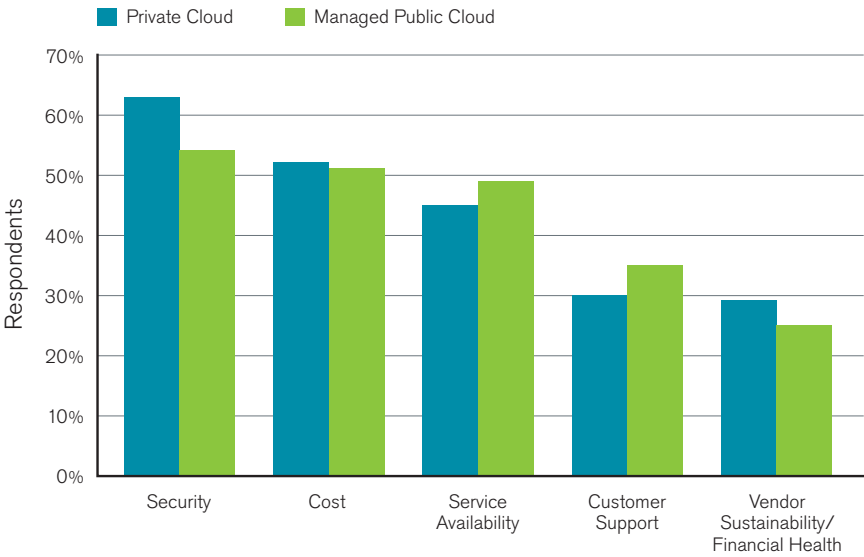
Volumetric and application-layer DDoS attacks

³ www.cnn.com/2009/TECH/12/24/cnet.ddos.attack/index.html

Cloud Services and Internet-Facing Data Centers Are at Risk

Today's IT industry is buzzing with all kinds of information and marketing related to "cloud" services. Once considered esoteric, cloud services are fast becoming part of normal computing environments and are expected to grow in the future. For example, the analyst firm Yankee Group estimates: "Enterprise cloud services generated U.S.\$9.2 billion in revenue worldwide in 2010, and forecasts that number to grow to U.S.\$22.3 billion in 2014, a CAGR of 30 percent."³

But these numbers could be even larger if it weren't for the security and availability concerns of enterprise customers. The chart below shows the results of a Yankee Group survey that asked enterprises, "What are your five main attributes when choosing a cloud service provider or partner?"

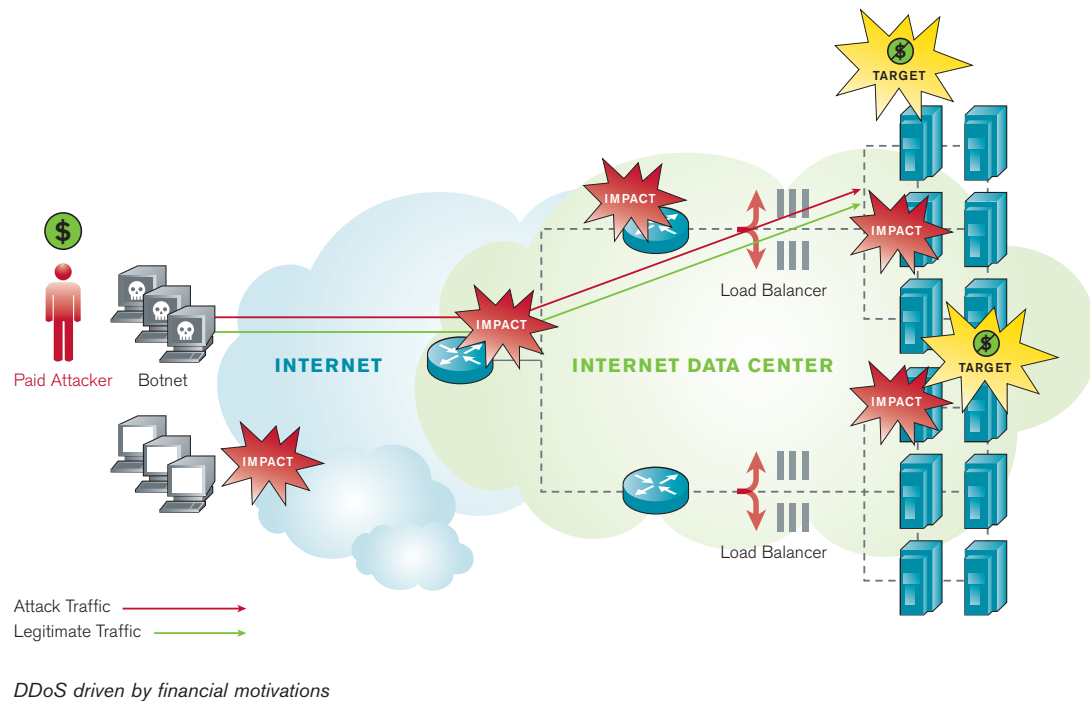


Security is a requirement for cloud services
Source: Arbor Networks, Inc.

As the chart clearly shows, security and availability are major concerns for enterprises. Therefore, it behooves service providers who offer (or plan to offer) cloud services to convince their prospects that they have the ability to secure and maintain the availability of their (and their customers') business services.

Data centers lie at the heart of every service provider's cloud service. Not surprisingly, enterprises and Internet data center (IDC) operators are very concerned with the availability of the critical services running in their data centers. But are these concerns warranted? Absolutely. Today's attackers view Internet-facing data centers as one of the new prime targets and are constantly launching DDoS attacks against these infrastructures for financial gain.

³ 2011 Enterprise Cloud Services Forecast: Revolution or Evolution, Cloud Is Moving Fast—January 10, 2011, Yankee Group



Attackers find Internet data centers attractive for the following reasons:

- The shared resources and multi-tenant nature of IDCs allow attackers to cause much collateral damage. In other words, they get “more bang for the buck!”
- Many times IDCs are running high-profile, mission-critical applications. This makes them ripe targets for extortion. By targeting such data centers, attackers are simply following the old saying “go where the money is.”
- Virtualization is a big part of data centers. This not only brings benefits but also opens up a whole new set of security challenges. For example, how do you get visibility into the virtual environment to protect it from inter-VM (virtual machine) attacks?

Stopping Volumetric and Application-Layer DDoS Attacks

To summarize thus far:

1. Attacks are getting larger (i.e., volumetric attacks are getting bigger).
2. Attacks are getting more sophisticated (i.e., new application-layer attacks or combined volumetric and application-layer attacks are becoming more common).
3. Data center attacks are getting more frequent (i.e., multi-tenant, Internet-facing data centers are becoming the new prime targets for attackers).

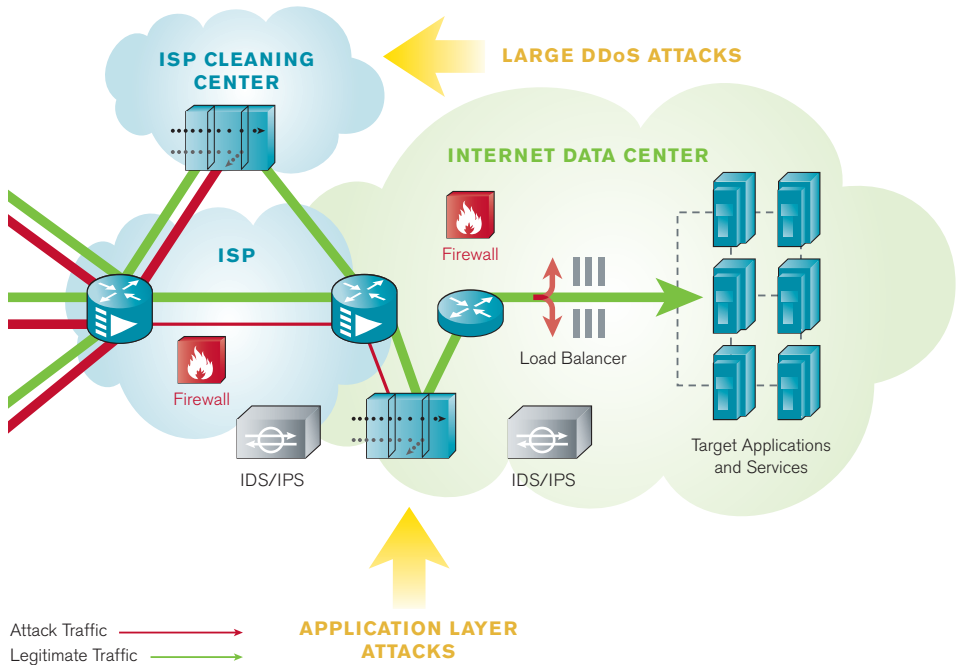
With that in mind, today may be the most challenging time ever faced by data center operators and security teams. Fortunately, there are best practices and products such as Intelligent DDoS Mitigation Systems (IDMS) that service providers can rely upon to help maintain the availability and security of their business services.

A Layered Approach and the ISP's Role

Today's attacker uses a combination of 1) volumetric and 2) application-layer attacks to execute multi-vector threats. To stop both of these attacks, you need to take a layered approach. That is, you must offer a combination of network-based (in the ISP's network or "cloud") and data center-based DDoS attack detection and mitigation.

Industry best practices have proven that:

- 1. The best place to stop volumetric DDoS attacks is in the ISP's cloud (via network-based DDoS protection).**
By the time the attack reaches the data center, it's usually too late to mitigate because it has already overwhelmed the network infrastructure or security devices (i.e., in-line firewalls and IPS). You must rely on the network-based DDoS protection of your ISP to stop these types of attacks.
- 2. The best place to perform application-layer DDoS detection and mitigation is in the data-center edge.**
Because these attacks are usually much smaller than volumetric attacks, they are harder to detect and stop in the ISP's network. A data center edge-based DDoS protection system gives operators the ability to customize detection and mitigation for the unique applications running in their data center.



Multiple layers of defense required for comprehensive DDoS protection

Since today's DDoS attacks require detection and mitigation capabilities both in an ISP's network and in the data center, it's easy to see how an ISP can deliver a valuable and comprehensive DDoS protection service to customers. If you are not an ISP, speak with your ISP(s) about how best to deploy such a managed security service. For example, you could take a hybrid approach where the ISP offers network-based DDoS protection for volumetric attacks while the data center operator handles data center-based protection for application-layer attacks.

Why Firewalls and IPS Fail to Stop DDoS Attacks

Today, many security teams mistakenly rely on traditional security products such as firewall and IPS devices to protect themselves from DDoS attacks. Though these devices are essential elements of the well-known Information Security Triangle that seeks to protect the confidentiality, integrity and availability of data and services, they cannot stop all DDoS attacks. In fact, they can make matters worse. IPS devices, for example, block break-in attempts that cause data theft. Meanwhile, a firewall acts as policy enforcer to prevent unauthorized access to data. While such security products effectively address network integrity and confidentiality, they fail to address a fundamental concern regarding DDoS attacks—network availability. What’s more, IPS and firewall devices are configured to allow the exact protocols that hackers use for attacks (i.e., TCP port 80). Since they are “stateful”, inline solutions, these devices are vulnerable to DDoS attacks and often become the targets themselves. The table below provides other reasons why traditional on-premise security products such as firewall and IPS devices do not offer adequate DDoS attack protection.



Key elements of an information security strategy

Why Existing On-Premise Solutions Fail to Address DDoS Security	
Vulnerable to DDoS attacks	<ul style="list-style-type: none"> - Because these devices are in-line, stateful devices, they are vulnerable and targets of DDoS attacks. - First to be affected by large flood or connection attacks.
Complicated to use	<ul style="list-style-type: none"> - Require skilled security experts. - Demand knowledge of attack types before attacks.
Failure to ensure availability	<ul style="list-style-type: none"> - Built to protect against known (versus emerging) threats. - Designed to look for threats within single sessions, not across sessions.
Protection limited to certain attacks	<ul style="list-style-type: none"> - Address only specific application threats. - By default, they must allow common attack traffic such as TCP port 80 (HTTP) or UDP port 53 (DNS). Do not handle attacks containing valid requests.
Deployed in wrong location	<ul style="list-style-type: none"> - Very close to servers. - Too close to protect upstream router.
Incompatible with cloud DDoS protection systems	<ul style="list-style-type: none"> - Fail to interoperate with cloud DDoS prevention solutions. - Increase time for response to DDoS.

The Solution: Layered Intelligent DDoS Mitigation Systems (IDMS)

The limitations in IPS devices and firewalls reveal the key attributes required in an IDMS solution. An IDMS must be “stateless.” In other words, it must not track state for all connections. A stateful device is vulnerable to DDoS and will only add to the problem. The IDMS solution must also support various deployment configurations; most importantly, it must allow for out-of-band deployments when needed. This deployment flexibility can increase the scalability of the solution, which is a requirement as the size of DDoS attacks continues to increase.

To truly address “distributed” DoS attacks, an IDMS must be a fully integrated solution that supports a distributed detection method. IPS devices leveraging single segment-based detection will miss major attacks. Moreover, an IDMS solution must not depend on signatures created after the attack has been unleashed on the targets; rather, it must support multiple attack countermeasures.

As mentioned previously, a layered approach is recommended to detect and stop both volumetric and application-layer DDoS attacks. Therefore, the ideal IDMS should be able to support both a network-based (in the ISP's cloud) and a data center-based deployment. In addition, both the ISP cloud-based and data center-based IDMS devices should be able to communicate with each other to coordinate mitigations during a multi-vector attack.

Finally, an IDMS must provide comprehensive reporting and be backed by a company that is a known industry expert in Internet-based DDoS threats.

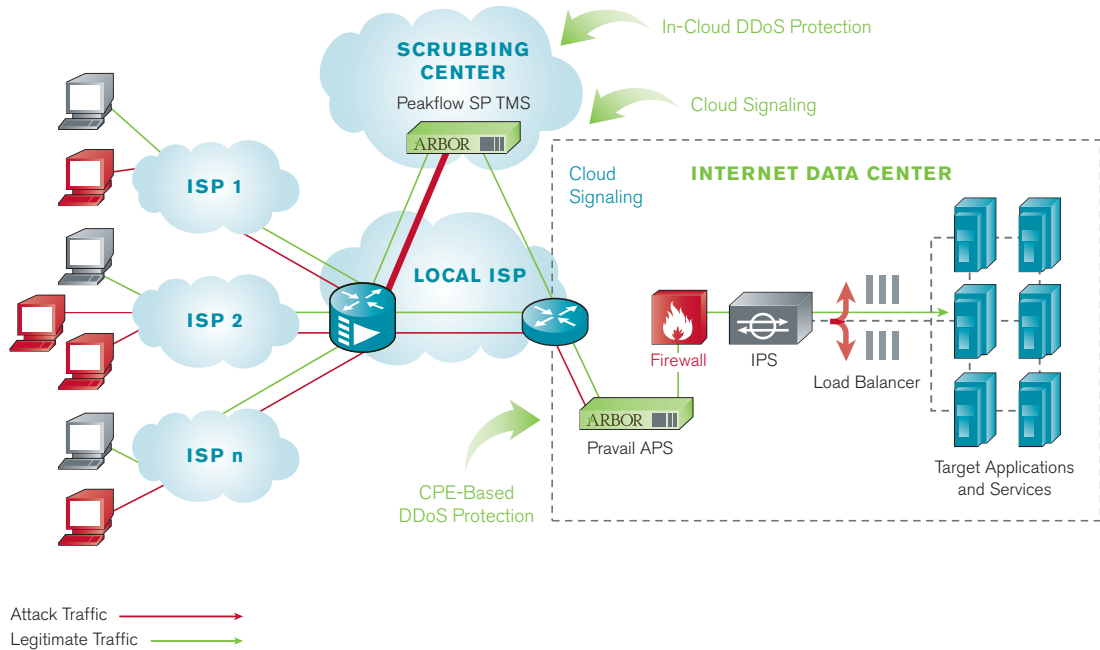
The table below summarizes the key features of IDMS.

Key Features of an IDMS Solution
Stateless
Inline and Out-of-Band Deployment Options
Scalable DDoS Mitigation
Ability to Stop "Distributed" DoS Attacks
Multiple Attack Countermeasures
Comprehensive Reporting
Support of Both Network and Data Center-Based Deployment, with Active Communication
Industry Track Record and Enterprise

Arbor's Solution for a Layered DDoS Protection Service

Arbor Networks® has been in the business of Internet-based threat analysis since 2000. During this time, Arbor has gained a reputation as being an industry leader in botnet/DDoS attack analysis, detection and mitigation. Today, Arbor offers the following network security solutions:

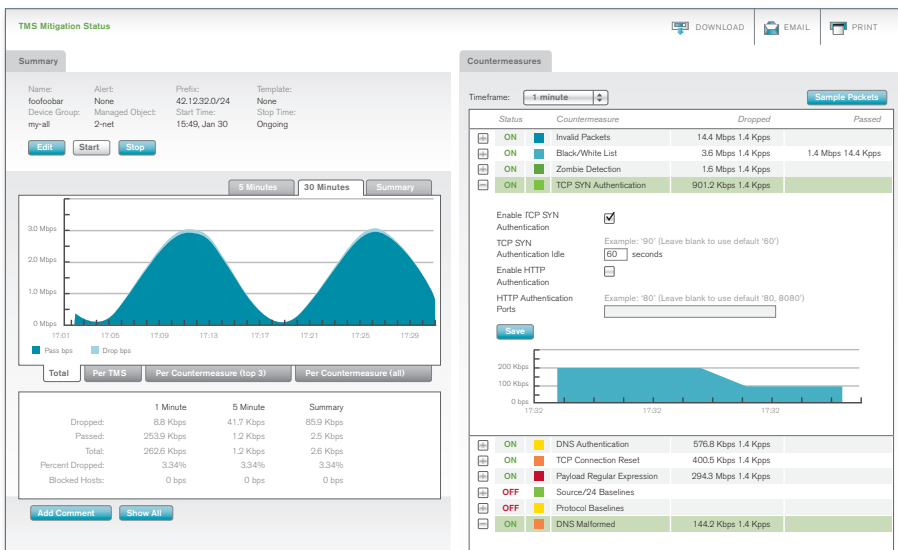
- **Arbor Peakflow SP solution ("Peakflow SP") and Arbor Peakflow SP Threat Management System ("TMS"):** Today, a majority of the world's ISPs rely on Peakflow SP and TMS to help protect their network infrastructure and deliver network-based DDoS protection services to their customers. Together, Peakflow SP and TMS offer an ideal network-based IDMS.
- **Pravail Availability Protection System ("Pravail APS"):** To help protect data centers against DDoS attacks, Arbor offers the Pravail APS.
- **Cloud SignalingSM:** By combining its solutions, Arbor offers a powerful capability known as Cloud Signaling, which allows a data center-based Pravail APS appliance to actively communicate with a network-based Peakflow SP and TMS deployment—enabling a comprehensive, layered DDoS protection solution. The next few pages highlight some of the key features of each of these products.



Arbor Networks' layered DDoS protection solution

In the ISP's Cloud: Arbor Peakflow SP and Threat Management System (TMS)

The combination of Peakflow SP and TMS is the ideal in-cloud IDMS solution for DDoS mitigation. As the first network-based system to extensively integrate carrier-class threat mitigation with threat detection, TMS can stop both volumetric and application-layer attacks without interrupting the flow of legitimate traffic in an ISP's cloud. The TMS 4000 appliance easily expands from 10 Gbps to 40 Gbps of surgical mitigation for network and application-layer attack countermeasures for HTTP(s), SIP and DNS—enabling it to address the growing and evolving DDoS threat.



The Peakflow SP and TMS solution also offers a large set of reports for comprehensive DDoS attack analysis. The solution also has many features that are designed to enable a managed network-based DDoS protection service.

Real-time alerting and mitigation dashboard

In the Data Center: Arbor Pravail Availability Protection System (APS)

Pravail APS focuses exclusively on stopping availability threats such as DDoS attacks. Data center operators can deploy Pravail APS in front of services to stop application-layer attacks and disrupt botnet communications.

With Pravail APS, a data center operator can:

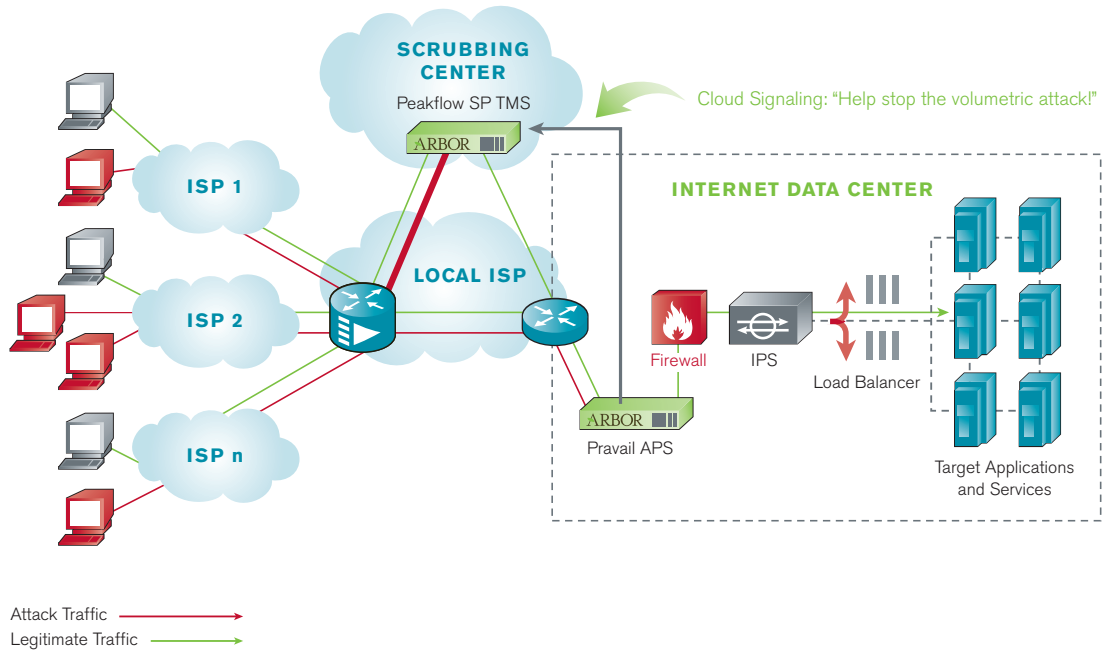
- Detect and block emerging application-layer DDoS attacks.
- Deploy a turnkey solution to stop threats immediately.
- Accelerate responses to DDoS attacks to prevent legitimate services from going down.
- Prevent illegitimate botnet communications by leveraging real-time security intelligence from Arbor's Active Threat Level Analysis System (ATLAS®).
- Mitigate volumetric attacks by coordinating with Cloud Signaling-enabled providers.



Pravail APS application-layer visibility and security

The Active Link Between the Cloud and the Data Center: Cloud Signaling

Because many volumetric attacks (i.e., those greater than the available bandwidth) cannot be stopped on premise, they require ISPs to mitigate the attacks in their network (in-cloud). At the same time, many cloud-based DDoS services cannot efficiently or quickly detect and stop lower-level application DDoS attacks. As a result, data center operators need a comprehensive DDoS solution with both cloud and on-premise protection to ensure optimal availability. Cloud Signaling is the glue that binds such a solution. By facilitating the communication from the on-premise Pravail APS appliance to the cloud-based Peakflow SP and TMS solution, the data center operator can shorten the time to resolution for DDoS attacks.



The bridge between cloud-based and premise-based DDoS protection

Conclusion

There's no doubt that as DDoS attacks become easier to execute, they will continue to increase in size, frequency and complexity. Though IPS devices and firewalls are effective tools in addressing network integrity and confidentiality, when it comes to DDoS protection, they provide a false sense of security and are inadequate at protecting network availability. To defend data centers against today's volumetric and application-layer attacks, one must take a layered approach and deploy Intelligent DDoS Mitigation Systems (IDMS) in both the ISP's cloud and the data center. This provides ISPs with a unique opportunity to offer their customers a high-valued, comprehensive DDoS protection service. ISPs (or other Managed Security Service Providers) can rely on Arbor's Peakflow SP, Threat Management System (TMS), Pravail Availability Protection System (APS) and Cloud Signaling capabilities—as well as Arbor's industry-recognized expertise—to deliver such comprehensive DDoS protection solutions.

For more information about the Peakflow SP, TMS and Pravail APS solutions, visit the Arbor Networks Web site www.arbornetworks.com or contact an Arbor representative at www.arbornetworks.com/contact.



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

Copyright ©1999-2011 Arbor Networks, Inc.
All rights reserved. Arbor Networks, the
Arbor Networks logo, Peakflow, Pravail, Cloud
Signaling and ATLAS are all trademarks of
Arbor Networks, Inc. All other brands may be
the trademarks of their respective owners.

WP/IDMS/0811

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for next-generation data centers and carrier networks. Arbor's proven solutions help grow and protect our customers' networks, businesses and brands. Arbor's unparalleled, privileged relationships with worldwide service providers and global network operators provides unequalled insight into and perspective on Internet security and traffic trends via ATLAS—a unique collaborative effort with 100+ network operators across the globe sharing real-time security, traffic and routing information that informs numerous business decisions.

For technical insight into the latest security threats and Internet traffic trends, please visit our Web site at arbornetworks.com and our blog at asert.arbornetworks.com.