Arbor White Paper

The Enterprise Guide to DDoS Protection

ARBOR® NETWORKS

About Arbor Networks

Arbor Networks, Inc. is a leading provider of network security and management solutions for enterprise and service provider networks, including the vast majority of the world's Internet service providers and many of the largest enterprise networks in use today. Arbor's proven network security and management solutions help grow and protect customer networks, businesses and brands. Through its unparalleled, privileged relationships with worldwide service providers and global network operators, Arbor provides unequalled insight into and perspective on Internet security and traffic trends via the ATLAS® Active Threat Level Analysis System. Representing a unique collaborative effort with 250+ network operators across the globe, ATLAS enables the sharing of real-time security, traffic and routing information that informs numerous business decisions.

The DDoS Situation

Enterprise security teams must deal with a broad assortment of security attacks that seek to steal data, cause service outages and wreak havoc on the network. Distributed denial of service (DDoS) attacks are nothing new, but their frequency and sophistication have drastically increased in the past few years.

Quite simply, DDoS attacks are now part of the advanced threat landscape, with attack types varying by size, vector and desired outcome. Many security products claim to provide DDoS protection, but how effective are they? This paper outlines the challenges of DDoS attacks and describes the features you need in a DDoS prevention solution to more effectively protect your network from these threats.

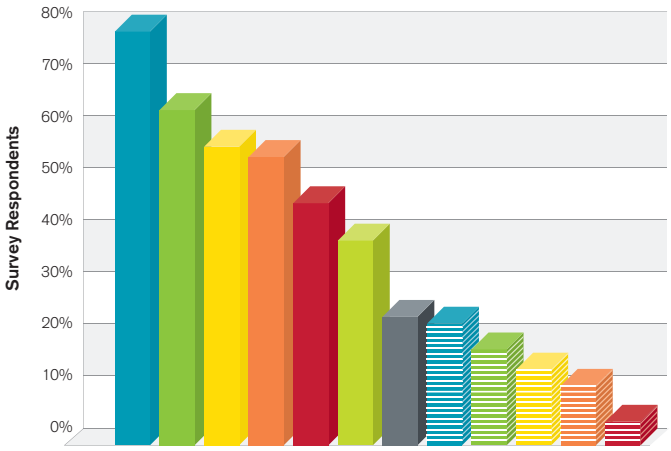
As a security professional, you've got a tough job right now. Most likely you are dealing with a constant stream of fast-changing attacks that make it difficult—if not impossible—to understand their triggers, profiles or effects. If you are not successful at blocking these attacks, confidential information may be accessed or stolen, valuable services may not be available to employees or customers, revenue may be lost and your company brand may be hurt.

How Prevalent Is DDoS?

According to Arbor's 2012 *Worldwide Infrastructure Security Report:*

- Four of the top five operational threats seen over the last 12 months are DDoS-related.
- The top four perceived operational threats for the next 12 months are DDoS-related.
- In a 60 percent increase over last year, nearly half of respondents are seeing multi-vector attacks.
- HTTP and DNS are the services most frequently targeted by application-layer attacks.
- 83.3 percent of data center respondents now see between one and 50 attacks per month.

Most Significant Operational Threats



- **76%** DDoS Attacks Toward Customers
- **61%** Infrastructure Outage (Partial or Complete) Due to Failures or Misconfiguration
- **54%** DDoS Attacks on Services (DNS, Email)
- **52%** DDoS Attacks Toward Infrastructure
- **43%** Infrastructure Outages (Partial or Complete) Due to DDoS Attack
- **36%** Botted/Compromised Hosts on Service Provider Network
- **21%** Under-Capacity for Bandwidth
- **20%** Botted/Compromised Hosts on Corporate or Command and Control Network
- **15%** Advanced Persistent Threat on Corporate or Command and Control Network
- **11%** Malicious Insider
- **8%** Industrial Espionage or Data Exfiltration
- **2%** Other

Source: Arbor Networks, Inc.

According to the Arbor Networks *Worldwide Infrastructure Security Report,* DDoS attacks were a significant operational threat in 2012.

The motivation behind DDoS attacks has evolved. These attacks are no longer just single hackers trying to take down top name sites in the name of publicity. Instead many of these attacks are being organized by "hacktivist" groups and are geo-politically targeted or aimed at competitive takeouts.

Most security professionals realize that security issues can't be fixed with a single "silver bullet" solution. However, complex technologies that only handle single issues or products that don't easily adapt to changing security needs are a source of frustration, as well as a drain on precious resources.

So what IS needed to better protect enterprises from DDoS attacks? Based on feedback from Arbor customers and prospects, we've identified the following five enterprise needs with regard to security—and more specifically, denial of service.

I Don't Want to Deal with DDoS Threats at All. I Want My Service Provider to Block Them Before They Reach Me.

A clean-pipes service from your ISP or cloud DDoS provider is often the first step to addressing DDoS attacks and should be part of a full solution. However, cloud-based DDoS services are usually reactive and don't offer protection from application attacks. In such cases, this means enterprises must suffer the attack for a minimum of 45-60 minutes before the service provider can identify it and respond with appropriate protection.

Application attacks represent a particular weak spot for cloud-based services. Such services don't understand your specific applications. What's more, their sampling of network traffic almost always misses today's low-and-slow application-layer DDoS attacks. Protection from application attacks requires an "always-on" defense, which often comes from a perimeter-based DDoS solution.

While real-time protection is required for blocking application DDoS attacks, perimeter-based protection can only block traditional volumetric DDoS attacks up to the capacity of the Internet connection. For example, a perimeter solution deployed on a 10GE network should block DDoS attacks with aggregate traffic of up to 10 Gbps, but only cloud and ISP-based solutions can handle attacks that surpass the capacity of the incoming pipe.

A DDoS solution must integrate ISP-based protection against volumetric attacks and always-on protection for application DDoS attacks. Recent advanced and highly targeted DDoS attacks integrated both application DDoS and volumetric DDoS techniques. With aggregate traffic of more than 50 Gbps, ISP-based defenses successfully blocked more than 80 percent of the bad traffic. But this left more than 8 Gbps of attack traffic that had to be blocked at the perimeter. Enterprises that had an integrated ISP and perimeter solution were able to stay online—even during the peak of the attacks.

I Need a Security Solution That Doesn't Buckle Under the Pressure of Constant Attacks.

A dirty secret of the network security industry is that certain perimeter solutions (firewalls, IDS/IPS) can actually be taken offline during a DDoS attack. In fact, perimeter security can be the target of a DDoS attack and the source of network failure.

Perimeter devices like IPS and firewalls have a solid place in the security infrastructure of the enterprise. They provide protection from known attacks and control access to internal networks. However, firewall and IPS devices are "stateful," which means they keep track of certain attributes of network traffic to determine that it is legitimate and not attack traffic. The ability to keep session state is a key feature that makes these products valuable—but it is also what makes them vulnerable to being taken offline during a DDoS attack.

For example, some DDoS attacks have been known to cause high-performance 10GE firewalls to fail by simply sending less than 100 Mbps of invalid TCP packets. Once perimeter devices fail, enterprises face the tough decision to either go dark and fail closed or fail open with no security in place, which runs the risk of exposing sensitive systems and losing critical data.

To be effective against DDoS, organizations need a solution designed for the job. Firewalls and IPS devices may offer a few DDoS features, but they are not a viable solution.

> **"Without a doubt, the number-one driver for the DDoS prevention market is the attacks themselves. From the Iranian elections, to Wikileaks and the Anonymous army attacking anything with a whirring fan, DDoS attacks have been big news for the last 2 years."**
>
> **DDoS Prevention Appliances, Analysis from Infonetics Research, June 2012**

I Need a Fix for <Fill in Latest Security Attack> and I Need It Now!

Attacks on enterprise networks are constantly changing. And often they are a blend of different attacks specifically designed for the organization they are targeting. These can range from DDoS attacks designed to take out first-line perimeter defenses (as outlined previously) all the way down to socially-engineered spam emails designed to amass hosts for a botnet. DDoS attacks alone come in a variety of techniques and methodologies that evolve to take advantage of new infrastructures, new protections and new data sources. Businesses need a solution that provides broad protection and can keep up with the latest attacks.

My Boss Won't Approve a Security Purchase If It Impedes Business Operations.

Security—like any form of enterprise control—is an interesting paradox. By preventing malicious activity, a security solution may prevent some legitimate actions as well. Some organizations are willing to accept this risk if it means that the network will run unimpeded or employees can download whatever tools they need to do their jobs. Where is the line? Organizations need security products that limit risk of catastrophic data loss or outage, but these security solutions must also be aligned with—and supportive of—business operations.

I Need an Intelligent DDoS Solution That Can Understand My Applications and How They Operate.

Network security solutions are designed to protect the network. However, in a world where applications are the face between an organization and its constituents, understanding application behavior is essential for network security components. Without intelligent application awareness, network security tools can be more of a hindrance to service availability or behavior. The lack of application intelligence is often a weakness of cloud-based DDoS solutions because they approach every client as if their applications were exactly the same. Organizations need a solution designed specifically for protecting applications from availability threatening attacks.

While these traditional security and network tools have a few "check-the-box" features, DDoS can't be addressed with a handful of IPS signatures. The very nature of DDoS requires a solution that scales with the network and is itself immune to DDoS threats. For this reason, enterprise security teams are deploying dedicated DDoS prevention appliances.

Several factors separate DDoS prevention products from traditional network security tools. When selecting protection from DDoS threats, please consider the following critical features that differentiate a true DDoS solution from a network security tool that includes DDoS protection.

How Does Your Security Vendor Stack Up Against DDoS?

Selecting a vendor to help protect your organization from the devastating effects of denial of service requires serious evaluation. For pure "availability," load balancers, which allow you to spread traffic among several network points can help keep service going. However, it's not fixing the problem. Similarly, many network security products claim DDoS detection and blocking as a feature of their products. Again, this does not adequately address the problem. DDoS is an evolving and dangerous advanced threat that requires a product designed specifically for availability protection.

Stateless Inspection

In-line perimeter devices, such as firewalls or IPS, use stateful inspection to block attacks that threaten the integrity or confidentiality of data. While stateful inspection is useful for identifying certain threats, it leaves the device open to attack and outage. DDoS attacks can take advantage of a security device that uses stateful detection and overwhelm its "state," rendering it useless. Attackers have then taken your first line of defense offline, and in the process, have inhibited network function.

Automatic Protection for Application-Layer Attacks

The application layer of the network includes Web servers, which are often the primary interface a company uses to communicate with its customers. For retailers, financial institutions or any online enterprise, this is also the source of revenue. Unfortunately, the application layer is an increasingly popular target for organized attackers. That's because these attacks fly below the radar of provider-based DDoS services and don't require the excessive bandwidth and resources of a 10, 50 or 100 Gbps attack. Quite simply, a single hacker with a small botnet can execute these attacks with a high degree of success—unless a dedicated DDoS solution is in place.

Always-On Integrated with Cloud Scrubbing

DDoS attacks are not typically a one-off event. They often incorporate a variety of attacks—ranging from volume-based attacks designed to take out all service, to coordinated lower-volume attacks designed to take out perimeter applications. An ideal DDoS prevention solution should not only provide on-premise DDoS protection to identify and block targeted attacks, it should also include ways for the organization to work with upstream providers. Because SP-based services require 45-60 minutes before mitigation, enterprises that can't afford that outage require an always-on solution. When large volumetric attacks do occur, the perimeter device should provide some mitigation, while accelerating the process of engaging the cloud-based DDoS protection from the SP.

Intelligent Identification of Web Crawlers

Advanced techniques in search marketing have created an additional challenge for security professionals. Major search engine vendors use custom Web crawlers to mine enterprise Web sites for information or terms used to rank or place these enterprise sites during a search. However, many of these Web crawlers look and behave like bots, creating some confusion and possible false positives from traditional security products. To prevent the corporate Web page from sinking in search rankings, a DDoS prevention solution should be able to easily identify legitimate search engine Web crawlers and—as a policy—not block their access to the site.

Packet Capture and Custom Policy Creation

DDoS is a strange beast. It comes in so many types and sizes. As highlighted in recent attacks from Anonymous, DDoS can be highly customized to target your specific network. In these instances, you don't have time to figure out how to create a custom attack policy. You need to stop the attack immediately. If DDoS prevention is simply a feature of a network security product, this type of protection is often an afterthought that's been added to the product, and can be clunky and not intuitive. A true DDoS prevention solution can easily identify and capture bad packets, and then immediately use that information to create—and deploy—a custom attack policy to protect your network.

Bot Detection and Mitigation

To be valuable at the perimeter, a security device must not only detect bot activity, but understand the dynamics behind the bot. Most security devices can detect bot activity, but are not equipped to understand how the bot behaves. As a result, they provide "blanket" protection that can inadvertently impede business operations. Because bot behavior can change depending on who is handling command and control, it is important to be up-to-date on the latest security attacks and bot information. A true DDoS prevention solution should be continuously updated to detect and block traffic from the latest botnets.

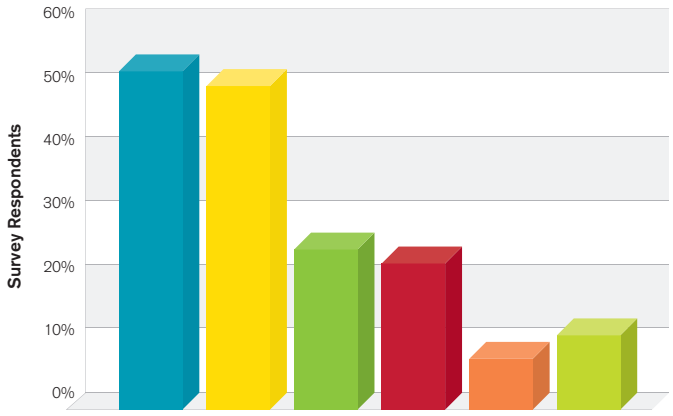
Asymmetric Traffic

Most enterprise data centers rely on at least two ISPs. With this and other redundancies, a security appliance deployed at the network edge is not guaranteed to see both the inbound and outbound traffic of a single connection. For this reason, a DDoS solution must be effective at blocking attacks in these environments by supporting asymmetric networks.

CDN and Proxy-Aware

Once malicious traffic is identified, you can block DDoS attacks at high speeds by simply dropping malicious packets or by temporarily blocking all traffic from the attacker's IP addresses. But if the attack targets your network through a CDN or proxy, the attacker's real IP addresses can be hidden. If the DDoS solution ends up blacklisting the CDN's IP address, your "protection" has just amplified the attack and taken all legitimate traffic offline. For this reason, DDoS solutions must first recognize proxies and CDNs, and then provide the necessary protection (and visibility) without impacting legitimate traffic.

Internal Network Security Threats



- **50%** Botted or Otherwise Compromised Hosts on Corporate Network
- **48%** Under-Capacity for Internet Bandwidth (Due to DDoS or Other Specific Event)
- **22%** Advanced Persistent Threat (APT) on Corporate Network
- **20%** Malicious Insiders
- **5%** Industrial Espionage or Data Exfiltration
- **9%** Other

Source: Arbor Networks, Inc.

According to the Arbor Networks *Worldwide Infrastructure Security Report,* half of the respondents found botted or compromised hosts on their network.

The Arbor Difference

The Pravail® Availability Protection System ("Pravail APS") from Arbor Networks meets the needs of the enterprise by helping to provide immediate protection from multiple types of DDoS attacks. With Pravail APS and integrated Cloud Signaling™ functionality, organizations can be more confident that their critical systems will be available for end users, employees and partners. Pravail APS includes the following features that specifically address the unique needs of the enterprise.

Keep Your Network SAFE with Pravail APS

The foundation of Pravail APS is the Stateless Analysis Filtering Engine or SAFE. As the name suggests, 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. Further, Pravail APS has the power to do more mitigation or analysis since it does not have the processing overhead of stateful inspection.

The SAFE architecture also enables Pravail APS to identify asymmetric traffic for increased visibility and improved forensic capabilities. This essential packet engine detects patterns or attack signatures that indicate an attack. Armed with this information, it is easy to create or modify policies for better protection.

Global Threat Intelligence Drives DDoS Protection

Security threats can change at a rapid pace to better infiltrate your network. As a security professional, your job is to protect the integrity of the business—not to be an expert on every attack or threat that exists in the world.

Arbor customers rely on Arbor's Security Engineering & Response Team (ASERT). This team is a dedicated security research group comprised of experts in attack analysis, security research and reverse engineering. ASERT actively manages the Active Threat Level Analysis System (ATLAS), a global network of data from more than 250 ISP deployments, plus a network of sensors strategically placed in front of several tier 1 service providers to collect attack data.

ASERT provides analysis on a broad range of security threats, including botnets which account for a majority of the DDoS attacks on the Internet today. On a daily basis, ASERT gathers more than 25,000 botnet samples. When new botnets or other DDoS attacks are discovered, ASERT creates countermeasures that are distributed to Arbor's Pravail APS via the ATLAS Intelligence Feed (AIF). This feed is updated regularly, providing accurate, effective protection against DDoS and maintaining critical availability of business applications.

Threat Updates That Block Today's Advanced Threats

ATLAS collects actual attack activity occurring in real time throughout the world. This data includes details such as where an attack is coming from and what it looks like. The ASERT teams uses this information to create botnet profiles and attack countermeasures that protect the enterprise from a broad selection of exploits such as malware, botnets and DDoS attacks.

Since the majority of business critical traffic uses Internet as a medium, accuracy is critical so that legitimate traffic is not blocked. Because AIF botnet protections and policies are created using real attack data from ATLAS, these countermeasures are among the most accurate in the industry. Further to this point, AIF also includes a "whitelist" of search engine web crawlers, so that they are not inadvertently categorized as bots. This level of accuracy not only improves security, but ensures the organization does not lose valuable ranking in search results.

Cloud Signaling℠ Offers Layered Security from the Perimeter to the Cloud

As the techniques for DDoS attacks advance and the motivations behind them evolve, data center operators need to find new ways for enhancing protection of their networks. Pravail APS provides organizations with an on-premise, always on protection against availability attacks. However, these organizations can strengthen this protection with targeted cloud scrubbing via the Cloud Signaling Coalition (CSC).

With cloud signaling, an enterprise that is under attack can package up critical details of that attack and send it to their SP or cloud provider for upstream protection.

Arbor is the only security vendor that enables enterprise organization to build a process for alerting SPs to DDoS attacks. Putting a process in place for sharing attack information with upstream providers enables organizations to create an intelligent, layered response for blocking attacks before they even reach the network perimeter.

DDoS Protection with a Business Focus

In addition to providing effective protection against DDoS, Pravail APS also offers detailed attack reporting in real time, making it easy for you to understand and demonstrate to upper management the actions taken by the appliance. Besides documenting these actions in audit logs, Pravail APS provides forensic reports detailing blocked hosts, origin countries of attacks and historical trends. You can use these easy-to-understand reports for compliance—or to educate management on the threats to service availability and the steps taken to address them.

Conclusion

Many of today's network security products claim to offer protection from DDoS attacks. However, not all DDoS protection is created equal.

Arbor Networks has specialized in DDoS protection for more than a decade. Its expert research team has an unparalleled view into this type of attack methodology and incorporates this data into true DDoS prevention for your network.

For more information, please visit www.arbornetworks.com.

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA +1 866 212 7267
T +1 781 362 4300

Europe
T +44 207 127 8147

Asia Pacific
T +65 6299 0695

www.arbornetworks.com

ARBOR® NETWORKS

WP/APS/EN/0213