Arbor White Paper

The Importance of On-Premise DDoS Protection

Why Today's Targeted DDoS Attacks Require a Strong Defense at the Enterprise Edge

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.

Table of Contents

Executive Summary

There was a time when distributed denial of service (DDoS) attacks threatened business operations by simply "flooding the network pipe" with traffic congestion. By overwhelming the connection to the Web server, these high-bandwidth "volumetric" attacks can take a Web property offline. In response, Internet Service Providers (ISPs) launched managed security services that provide enterprises with in-cloud DDoS protection. For nearly a decade, these in-cloud services remained an effective strategy for DDoS defense.

That all changed in 2010, when there was a dramatic shift in DDoS thanks to attackers who developed more sophisticated and targeted tools. Today, the application-layer is the most popular target for attacks, specifically Web services. These "application-layer attacks" generally consume less bandwidth and are stealthier in nature when compared to volumetric attacks, which makes them harder to detect. What's more, they can have a catastrophic impact on business availability by threatening critical HTTP, DNS, VoIP or SMTP applications and services.

Today's cloud-based managed security services are primarily effective at defending against volumetric DDoS attacks. The detection and mitigation of application-layer attacks requires an on-premise solution that's deployed at the enterprise perimeter. The question is, what type of on-premise solution is right for the job?

Unfortunately, many security organizations rely on perimeter-based security products such as firewalls and intrusion prevention systems (IPS) for this purpose—with unsuccessful results. That's because these devices "allow" the exact protocols (such as HTTP and DNS) that attackers use for application-layer DDoS attacks—enabling the attack to easily bypass what is often the first and only line of defense for an organization. In addition, because firewalls and IPS are stateful security devices, they are frequent targets of DDoS as attackers attempt to consume the connection state tables in these devices.

The Pravail® Availability Protection System ("Pravail APS") from Arbor Networks® is purpose-built for on-premise availability protection. This paper examines the DDoS evolution from volumetric to application-layer attacks, and describes how Pravail APS helps mitigate application-layer attacks before they impact network and service availability.

Evolution of DDoS: From Flooding to Application-Layer Attacks

DDoS attacks are rapidly evolving. Just a few years ago, DDoS was dominated by "volumetric" attacks that target and flood network connections. These high-bandwidth attacks usually originate from geographically distributed bots or compromised PCs grouped together into large-scale botnets. Some examples include the DDoS attacks against UK-based online betting sites[1] where the attackers extorted the gambling firms, and the politically motivated DDoS attacks against the Georgian government.[2] 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 addition to volumetric attacks, enterprises now face a new generation of DDoS attack that threatens business viability. Imagine a scenario, two days before Christmas and last-minute shoppers could not access some of the world's most popular Internet shopping sites. This happened a few years ago when a targeted DDoS attack against UltraDNS,[3] a leading provider of domain name system (DNS) services, took several major retail sites offline—at the height of the Christmas shopping season.

This incident revealed the potential impact of DDoS on e-commerce. More importantly, it exposed a new type of "application-layer" attack that is far more sophisticated, complex and dangerous. Aimed directly at the perimeter of enterprise networks or data centers, such attacks jeopardize the availability of Internet-facing businesses and services. These enterprise-focused attacks use less bandwidth than flooding attacks, making them harder to detect. They're also more specific in nature; application-layer attacks target existing stateful security infrastructure, such as firewalls and IPS devices, and can be used to shut down a particular Web site or Web-based service such as email, online banking or e-commerce.

Availability must be a core objective of enterprise security, especially when companies rely on critical services, such as Web, e-commerce, financial transactions, supply chain, email and VoIP. If key services and applications are down, business grinds to a halt. Today's attackers are well aware of this fact—and taking action. Armed with innovative new tools, attackers view Internet-facing data centers as their prime targets—and are increasingly deploying application-layer attacks to wreak havoc on business availability.

2004–2009

Botnets enable bandwidth-exhausting "volumetric" attacks against infrastructure (routers, DNS, name servers). In-cloud DDoS protection becomes essential.

2010 and Beyond

DDoS attacks have evolved substantially. New types of DDoS attacks are targeting the enterprise, including sophisticated "application-layer" attacks that target Internet data center services and enterprises. These low-and-slow attacks exhaust resources on the target and overload the server.

The motivation for DDoS attacks has changed as well. While making sites unavailable is a key driver in many attacks, DDoS attacks are being used as one component of a targeted, multi-vectored threat to wreak havoc on the enterprise. Stopping availability attacks before they can become a distraction is critical. On-premise DDoS protection is required.

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

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

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

The Search for the Right Solution

As DDoS attack tools become more sophisticated and easier to use, attackers are targeting applications—and bringing critical business services to a standstill. When this happens, organizations are under extreme pressure to find and fix the problem. Yet the tools to do so are often lacking.

Shortcomings of In-Cloud DDoS Managed Security Services

In-cloud managed security services provide an effective strategy for defending against high-bandwidth volumetric DDoS attacks. That's because the saturation occurs upstream and can only be remediated in the provider's cloud. However, relying exclusively on a cloud-based DDoS managed service leaves your network vulnerable to today's growing number of low-bandwidth application-layer attacks that can easily escape detection by cloud-based managed security services.

Why Firewalls and IPS Devices Fail to Stop DDoS Attacks

Firewalls and IPS devices are essential elements of a layered-defense strategy, but they are designed to solve security problems that are fundamentally different from dedicated DDoS detection and mitigation products. A firewall, for example, acts as policy enforcer to prevent unauthorized access to data. Meanwhile, IPS devices block break-in attempts that cause data theft.

DDoS is a different problem. DDoS attacks consist of legitimate traffic from multiple sources crafted to exhaust critical resources, such as link capacity, session capacity, application service capacity (e.g., HTTP and DNS) or back-end databases. Because such traffic is authorized and does not contain the signature content of known malware, it is not stopped by firewalls and IPS. As a result, these devices fail to address the fundamental concern regarding DDoS attacks—network availability. What's more, as inline, stateful inspection tools, firewalls and IPS devices are vulnerable to DDoS attacks, often becoming the targets themselves.

Cloud-Based DDoS Managed Services

Can Protect Against Volumetric or Flood Attacks

Because these attacks occur upstream, they are best remediated in the provider's cloud.

Cannot Detect and Mitigate Application-Layer Attacks

This type of attack can be very effective with as few as one attacking machine generating a low traffic rate. This makes them very difficult to proactively detect and mitigate without a purpose-built, on-premise device.

Cannot Protect Existing Infrastructure

Stateful security infrastructure such as firewalls/IPS are frequent targets of DDoS as attackers attempt to consume the connection state tables that are present in these devices. Even high-capacity devices capable of maintaining state on millions of connections can be taken down by these attacks.

Cannot Deal with Multi-Vector Attacks

Attackers are increasingly turning to multi-vector attacks that employ combinations of volumetric, state-exhaustion and application-layer attack vectors targeting an organization at the same time.

Superior Availability Protection with Pravail® APS

The Pravail Availability Protection System ("Pravail APS") from Arbor Networks is purpose-built for on-premise availability protection to help ensure reliable access to key network services. Pravail APS helps protect business continuity and availability from the growing constellation of application-level threats. It provides the world's most widely deployed DDoS detection and mitigation technology in an easy-to-operate appliance that is designed to automatically neutralize availability attacks before they impact critical services and escalate into costly and embarrassing outages.

Pravail APS uses stateless attack detection and filtering. This allows Pravail APS to remain functional during low-volume attacks that are designed to overwhelm and cripple stateful devices, such as firewalls and IPS.

In addition, Pravail APS delivers the following features and benefits:

"Out-of-the-Box" Protection

Easy to install, configure and use, Pravail APS provides immediate protection from application-layer DDoS attacks that threaten your service and application availability.

Proactive DDoS Detection and Mitigation

Pravail APS automatically detects and blocks DDoS attacks before service performance is impacted. Little to no user interaction is required, lessening the burden on your security team.

Visibility and Control

With Pravail APS, you gain real-time visibility into availability threats, attacks and blocked hosts.

Full Suite of Attack Countermeasures

Pravail APS incorporates advanced DDoS countermeasures that have proven effective in the world's largest and most complex network environments. These countermeasures include a set of packet-based protections developed by ASERT that helps neutralize the vast majority of global botnet threats.

Automated Threat Updates

Arbor has real-time visibility into more than 43Tbps of the world's Internet traffic. This unmatched insight enables Arbor to develop timely, automatic security updates to Pravail APS, keeping organizations one step ahead of emerging, malicious threats.

Combined On-Premise and Cloud-Based DDoS Protection

Arbor's unique Cloud Signaling™ capabilities seamlessly integrate the on-premise availability protection of Pravail APS with cloud-based DDoS protection delivered by many leading managed security providers who leverage Arbor's Peakflow® platform. Only Arbor can offer this type of comprehensive protection for the enterprise because of our pervasive service provider footprint. This integrated solution delivers the most comprehensive DDoS protection available today.

Real-Time Reporting and Forensics

Pravail APS produces in-depth, real-time attack reports that are easy to understand, along with forensics detailing blocked hosts, origin countries of attacks and historic trends.

The Role of On-Premise Solutions in DDoS Protection

A quick Internet search can identify a host of online banking and e-commerce sites victimized by DDoS attacks that could have been mitigated with the right on-premise solution. Here are a few recent examples.

Example 1: Availability Attacks on Mt. Gox

Tokyo-based Mt. Gox is the world's largest bitcoin exchange. Its trading platform executes 80 percent of all bitcoin trades in U.S. dollars and 70 percent of all trades in other currencies. Despite the fact that availability is critical to the company's ability to function, Mt. Gox outsourced availability protection—choosing a cloud-based managed security service provider for DDoS defense.

In April 2013, Mt. Gox became the victim of a DDoS attack "like we have never seen," reported the company. Aimed at manipulating the value of the bitcoin, the attack caused volatile swings in the price of the virtual currency, along with trading lags. According to Mt. Gox, the attackers intended to profit by selling their bitcoins at a high price, and then launching a DDoS attack to destabilize the exchange. When panic selling drove down the bitcoin's value, they would stop the attack, buy bitcoins at the lower price, and attack again when the price rose.

Even though Mt. Gox utilized a well-known, cloud-based MSSP for DDoS defense, they were still victimized by the one type of attack best mitigated in the cloud, a volumetric attack. By relying exclusively on their outsourced service provider, Mt. Gox was left vulnerable as the provider was, again according to Mt. Gox, "slower than usual to catch what happened."

On-premise DDoS protection would have enabled Mt. Gox to mitigate attacks as large as 10Gbps without the assistance of their cloud-based provider, maintaining control over their most valuable asset, availability itself.

Example 2: Multi-Vector Attacks on Bank Websites

Major U.S. bank Web sites were offline a total of 249 hours during a six-week period in 2013, perhaps the clearest indication yet that American companies are prime targets in an unrelenting, global cyber conflict.[4] These ongoing, sustained attacks against U.S. financial services firms are examples of "funded hacktivism" and demonstrate the importance of deploying best practices for defense if availability is important to your organization, as it is within financial services.

These were multi-vector attacks, combining—often at the same time—large-scale volumetric attacks, state exhaustion attacks against existing infrastructure like firewall/IPS devices and attacks against applications. The attack tactics observed were a mix of application-layer attacks on HTTP, HTTPS and DNS with volumetric attack traffic on a variety of TCP, UDP, ICMP and other IP protocols. Pravail APS provides organizations with on-premise, always-on protection against availability attacks, as well as attacks that can exhaust traditional perimeter security devices such as firewalls and IPS devices.

The other obvious and uncommon factor at play was the launch of simultaneous high-bandwidth attacks on multiple companies in the same vertical. This factor puts a strain on the mitigation infrastructure of certain managed security providers, and again highlights the loss of control when relying exclusively on cloud-based managed services.

[4] www.cnbc.com/id/100613270

Example 3: State-Exhausting Attacks

The largest DDoS attack in history—measured at 300Gbps—struck Spamhaus, an IP blacklisting service, in March of 2013. While 300Gbps is a staggering volume of Internet traffic, it is—for now—an anomaly. The average size of a DDoS attack in 2012 was 1.67Gbps.[5] This is a relatively small amount of attack traffic compared to 300Gbps, but it can have a major and detrimental impact on organizations that rely on firewall and IPS devices for on-premise security.

Such devices are not designed to address the DDoS problem. In fact, as stateful, inline tools, firewall and IPS devices are vulnerable to DDoS attacks, often becoming the targets themselves. Pravail APS enables on-premise mitigation of up to 10Gbps. And by using stateless attack detection and filtering, it stays up-and-running during low-volume attacks that can overwhelm firewalls and IPS devices.

Conclusion

Today, DDoS attacks tend to fall into one of three broad categories: volumetric attacks, application-layer attacks and state-exhaustion attacks.

The best place to stop volumetric DDoS attacks is in the ISP cloud because the saturation happens upstream and can only be remediated in the provider's cloud. However, relying exclusively on a cloud-based DDoS managed service leaves your network vulnerable to application-layer and state-exhaustion attacks. The best place to stop application-layer and state-exhaustion DDoS attacks that threaten network availability is at the enterprise perimeter using an on-premise solution because such attacks can only be detected and blocked at these locations.

Pravail APS from Arbor Networks is purpose-built for on-premise availability protection—better enabling you to mitigate application-layer and state-exhaustion attacks before they impact network and service availability.

[5] Arbor Networks eighth annual *Worldwide Infrastructure Security Report*

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/ONPREMISE/EN/0513