Stratecast | FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

Entering the Next Phase of DDoS Defense

Stratecast
Executive Brief

April 2012

www.frost.com

ENTERING THE NEXT PHASE OF DDOS DEFENSE

INTRODUCTION

Stratecast's assessment is that the adoption curve of DDoS mitigation systems is entering a stage of accelerating market demand. A principal reason for this is that having a web presence is growing in value and criticality regardless of an organization's size or industry vertical.

In early 2010, Stratecast examined several approaches to identifying and mitigating Distributed Denial of Service (DDoS) attacks. We segmented DDoS mitigation systems into three categories: appliances (single function and multi-function appliances such as Web Application Firewalls and IDS/IPS); ISP scrubbing platforms; and cloud-based scrubbing centers. Each category, we explained, has its pros and cons. As organizations differ across several vectors—susceptibility, attack consequences, existing security equipment, reluctance to outsource, budget, and availability of knowledgeable staff—a range of approaches is beneficial.

Over the past 18 months DDoS mitigation systems have advanced in variety and capabilities. Providers have broadened the market appeal for these systems, and the advancements they contain have been essential to keep pace with the evolution in DDoS attacks—which are growing in frequency, severity, attack targets, and sophistication.

While our discussions with DDoS mitigation system providers confirmed that market demand is growing, there are also indications that market adoption remains distant from a 'must have' status, even with organizations that have a business-critical web presence. Cost, uncertainty of system effectiveness, inability to quantify the consequences of a previous successful mitigation of large volume attacks while sustaining the system throughput for good normal traffic, and even outright denial that an attack is possible, have collectively restrained the pace of market adoption.

Stratecast's assessment is that the adoption curve of DDoS mitigation systems is entering a stage of accelerating market demand. A principal reason for this is that having a web presence is growing in value and criticality regardless of an organization's size or industry vertical. It follows that protecting the availability and reliability of an organization's web presence, whether that web presence is for revenue generation or business operations, is correspondingly growing in importance. A correlated reason for why we expect adoption to increase in DDoS mitigation systems is that miscreants are attracted to opportunities for personal gain—financial, political, and notoriety—at the expense of others. Furthermore, the availability of attacker tools is more plentiful and the means to launch an attack simplified. Not only are the potential rewards in staging a DDoS attack growing in volume and value, the means have become easier. Simultaneously, DDoS mitigation solutions, as described in this document, are continuing to advance and will effectively lower adoption barriers.

[1] Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

[2] *DDoS Mitigation to the Rescue* (BCS 4-4), March 2010.

DDOS ATTACKS INCREASING AND EVOLVING

The body of evidence on DDoS attacks, like the DDoS attacks themselves, is growing. During the course of our research, we located numerous creditable sources that track and analyze the nature of DDoS attacks. The conclusions drawn from these DDoS attack tracking sources paint a grim picture for organizations that do not take the threat of DDoS attacks seriously.

- DDoS attacks are increasing in number by 20% - 45% annually; with application-based DDoS attacks, by some measurements, increasing in the triple digit levels.
- Correspondingly, hacking via DDoS is one of the most prominent tools used by the hacker community, many times as part of a multi-technique strategy.
- New records on the size of volumetric DDoS attacks are reached yearly—a testament to DDoS perpetrators' unending efforts to saturate the network connections and front-end website infrastructure (firewalls, Intrusion Prevention Systems, and routers) of the largest websites.
- Incidents of DDoS attacks on eCommerce sites escalate during the period when website disruptions will cause the greatest economic harm—the fourth quarter.

The body of evidence on DDoS attacks, like the DDoS attacks themselves, is growing.

. . .

The conclusions drawn from these DDoS attack tracking sources paint a grim picture for organizations that do not take the threat of DDoS attacks seriously.

DDOS MITIGATION SYSTEMS ADVANCING

The last 18 months has also seen a continuous stream of refinements and advancements in DDoS mitigation systems, a trend we predict will continue. The key take-away for organizations that recognize that the status quo is no longer sufficient—for example, ignoring the potential of an attack; increasing network and website infrastructure to absorb illegitimate traffic; enrolling in expensive expedited filter and block services; or relying solely on primitive, cleaver-like techniques (e.g., Access Control Lists)—is that the time is ripe to explore options to ramp up their defenses against DDoS attacks.

From our discussions with DDoS mitigation system providers—including hardware appliance vendors and service providers—we categorized system advancements into three areas.

- **Multiple Layers of Defense** – The trend toward application-layer DDoS attacks is clear, and unlikely to reverse. This trend is not, however, an indication that network-layer or flow-based, volumetric attacks will cease. On the contrary, network-layer attacks will continue for the primary reason that they are still an effective attack method in rendering a website unavailable (e.g., by saturating Internet access links or network perimeter routers, firewalls, and IDS/IPS). Therefore, a multi-layer defense strategy is essential. This is easier to prescribe than accomplish. The foremost challenges are having sufficient visibility and context to detect a wide range of attack types without slowing the flow and

One of the hindrances in the adoption of ISP scrubbing platforms and cloud-based scrubbing centers is the unpredictable variable cost component.

. . .

What is needed to serve a broader market in defending against DDoS attacks is a balance between consultative and automatic mitigation steps and procedures.

processing of legitimate traffic; and then conducting mitigation in the most effective manner. Therefore, the concept of multiple layers of defense must contemplate all components that are in the critical path of online activities.

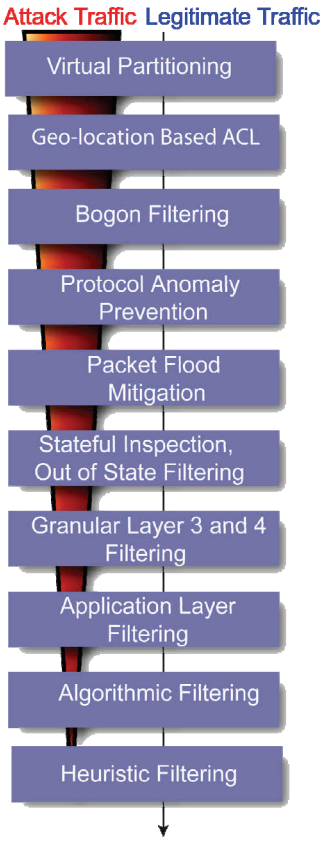
- **Cost Certainty** – One of the hindrances in the adoption of ISP scrubbing platforms and cloud-based scrubbing centers is the unpredictable variable cost component. Essentially, the more traffic processed, the greater the cost. With no reliable means to predict the frequency and size of network-layer attacks, organizations lack the cost certainty that they are accustomed to with other security systems. Full-time protection, with minimal or no cost surprises, needs to be the objective.
- **Automatic Attack Mitigation** – In consideration of the criticality of an organization's online operations, mistakenly blocking legitimate traffic is a DDoS mitigation failure, and a partial to full attacker success. Conversely, steps to minimize occurrences of false positives can also be problematic. For example, not every organization has the size, availability, and expertise in IT staff to huddle with a DDoS service provider to reach a mitigation decision or review DDoS appliance alerts in real time. Yet, 24x7 website availability is still critical. What is needed to serve a broader market in defending against DDoS attacks is a balance between consultative and automatic mitigation steps and procedures.

During our research, Stratecast assessed several DDoS appliance vendors and DDoS defense service providers along these three categories. Our review of Fortinet follows.

FORTINET REVIEW

Fortinet is a developer of DDoS attack mitigation appliances. Its customer base is diverse, encompassing enterprises, service providers of managed DDoS defense services, and web hosters.

In researching Fortinet, we spoke with three of Fortinet's customers: An unnamed online retailer;[3] Black Lotus, a provider of DDoS protection solutions, uses Fortinet to support its managed services customers; and ILK Internet GmbH, a full service Internet Service Provider based in Germany, uses Fortinet appliances to protect selected traffic by using routing policies in their core network and virtualization features of the appliance.



- **Multiple Layers of Defense** – The Fortinet appliances provide protection from both network-layer and application-layer attacks through a series of filters (see side bar). Situated in close proximity to an organization's web servers, Fortinet appliances examine bi-directional traffic; a critical capability in detecting application-layer attacks. Additionally, Fortinet appliances are equipped with ready-to-use policies to identify and block common or generic DDoS attack techniques and patterns.

  In addition to preventing DDoS attacks immediately, Fortinet's learning mode takes policy efficiency one step further by creating a profile of acceptable traffic patterns based on actual traffic. ILK Internet GmbH, for example, stated that in just two weeks of learning mode, it was able to refine policies to block highly customized attacks aimed at its website, without incurring the risk of blocking legitimate traffic. With web site functionality never being static and the same for attacker's efforts (if one means is blocked, they will try another), continuously learning and re-tuning of policies is essential. In similar fashion, Fortinet continuously updates its generic set of policies for what the company has learned from the experiences of its global customers. With learning mode and generic policy updates combined, Fortinet customers have two means to keep their DDoS defenses at peak performance.

  Other elements of Fortinet's multiple layers of defense include virtualization and geo-location blocking. With Fortinet's virtualization feature, policy administrators can establish up to eight independent policy domains in a single appliance. By utilizing this feature, attacks in one network segment will not impact other segments; and this feature also helps in reducing the need for replicated network segments.

  Fortinet appliances can block traffic based on geo-location through efficient hardware logic. Used judiciously, geo-location blocking can materially reduce the load on back-end servers by eliminating traffic from unwanted countries and regions (e.g., those regions that are outside a company's operational footprint).

- **Cost Certainty** – By design, an appliance approach to defending against DDoS attacks avoids the variable costs of a service, up to a point. If volumetric attacks exceed the appliance's processing capacity, the appliance owner may need to

[3] The online retailer's name is withheld for security reasons, that is, avoid unintentionally inviting attacks by fame-seeking hackers. For interested parties, this company is available for reference checks upon request.

...an appliance approach to defending against DDoS attacks avoids the variable costs of a service...

consider upgrading to a larger, more expensive appliance and increase its access bandwidth capacity; or augment the appliance with a network or cloud-based service that filters DDoS traffic in advance of the access link. Regardless of direction taken, the organization is faced with increasing DDoS protection expenditures. However, volumetric, network-layer attacks may not be the problem. Application-layer attacks, which are designed to over-consume the processing capacity of website infrastructure, and are not large consumers of access bandwidth, may be the problem. In this circumstance, an appliance approach with effective application-layer detection and attack countermeasures could be sufficient.

As shared by Black Lotus, Fortinet's dedication to upgrading its appliance software to address new forms of attacks and improve management efficiency was instrumental in selecting the company's appliances over other vendors' products. ILK Internet GmbH also cited Fortinet's ease of configurability as a point of differentiation in comparison to other vendors' products.

Previously stated, Fortinet appliances support virtual instances. This feature is not only beneficial in supporting multiple layers of defense but also is a cost containment and administration-friendly feature for organizations that have multiple web properties to protect, and that need unique policies for each. Virtual instances can also be effectively used in defense escalation. Rather than have a single set of policies, multiple sets can be defined in advance, such that the organization can apply a more stringent set of policies if the preceding policies were inadequate.

As shared by Black Lotus, Fortinet's dedication to upgrading its appliance software to address new forms of attacks and improve management efficiency was instrumental in selecting the company's appliances over other vendors' products.

Customer support is also crucial in defending against DDoS attacks. Even with the grandest of plans to outsmart the attackers, organizations acting on their own do come up short. In those instances, the support of the DDoS vendor is invaluable in assisting organizations in getting the most from their DDoS mitigation investments. ILK Internet GmbH recognized Fortinet for its accessibility and willingness to 'go deep' in providing technical assistance, all without sustaining additional charges.

- **Automatic Attack Mitigation** – Critical product attributes for the online retailer are protection from a broad range of attack types and automatic attack mitigation. Distinctive with this online retailer is that it also subscribes to a network-based DDoS mitigation service offered by its Internet Services Provider (ISP). This retailer has subscribed to this service for three years but the service does not align completely with its needs. For example and common with many businesses, having staff available to interface with the ISP when the ISP detects traffic anomalies is not feasible. Rather, this online retailer prefers the automatic mitigation of Fortinet. Although this online retailer will continue with its ISP DDoS protection service, there will be a shift in use. The Fortinet appliance will be primary in detecting and mitigating DDoS attacks. Using preset traffic thresholds, configurable by time of date, day of week, and season, the online retailer will communicate to the ISP when the threshold has been exceeded so countermeasures can be taken to avoid saturation of

the data center access link.

Also, it is not uncommon for online retailers, banks, and other entities with public-facing websites to have multiple Internet access links provided by multiple ISPs for the purpose of business continuity. For automatic attack mitigation, DDoS mitigation at the point of Internet access link convergence—that is, at the edge of the retailer's or bank's network—lessens the effort and potential expense of coordinating DDoS mitigation among multiple ISPs.

Stratecast
The Last Word

An underlying precept of the Internet is uninterrupted availability. Distributed Denial of Service attacks fracture this precept by intentionally restricting and outright blocking legitimate user access to targeted websites. The original method to accomplish this objective is to saturate the network infrastructure (e.g., network access, routers, firewalls, and IDS/IPS) with bogus traffic. Essentially, network-layer attacks block the gateways leading into websites. The more subtle and less voluminous but equally potent application-layer attacks skip through these gateways and overwhelm the website infrastructure with processing requests.

Fortunately, website owners are not powerless to fight back. As described in this document, DDoS mitigation providers are actively improving defensive systems, and Fortinet is a prime example. While staying ahead or even shoulder to shoulder with the hacker community is a never ending challenge, good effort is underway.

For website operators that have not yet given the risk and business impact of DDoS attacks serious consideration, this is perilous ignorance. Although there is no guarantee an attack will occur, there is also no guarantee that an attack will not occur. What can be stated with certainty is that the probability of a DDoS attack is rising. Furthermore, when consideration is given to the use of botnets to perpetrate DDoS attacks, the increasing number of independent Internet-connected appliances, and growth in machine-to-machine Internet interactions, this probability is marching toward a certainty.

For website operators that have not yet given the risk and business impact of DDoS attacks serious consideration, this is perilous ignorance.

Michael Suby

VP of Research

Stratecast | Frost & Sullivan

msuby@stratecast.com

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 STRATECAST

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 40 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.