IDC TECHNOLOGY SPOTLIGHT

Cloud Alternatives Provide New View on Cutting-Edge Attack Vectors

September 2015

Adapted from *Worldwide DDoS Prevention Products and Services 2014–2018 Forecast* by John Grady, Christina Richmond, and Christian A. Christiansen, IDC #251384

Sponsored by Fastly

Since 2012, IDC has seen a sharp increase in the frequency, bandwidth volume, and complexity of distributed denial-of-service (DDoS) attacks. As these attacks become more prevalent, organizations need to be aware of and take steps to protect their infrastructure from the advanced methods today's attackers use. DDoS defense is an extremely dynamic and evolving market. This IDC Technology Spotlight discusses the trends and considers the role of a content delivery network (CDN) such as Fastly's in the DDoS prevention market. A CDN allows for real-time control of and visibility into the traffic on an organization's site, providing a strong alternative to traditional DDoS prevention products. These capabilities provide a better strategy for managing threats in a distributed way.

Introduction

As DDoS attacks continue to increase in frequency and complexity, companies are starting to take notice of this specific attack vector and hope to mitigate it by using DDoS prevention techniques. The largest attack in 2013 was 400Gbps, approximately 100Gbps greater than the largest previously known attack. The market for standalone products is expected to grow from $461.8 million in 2013 to $944.4 million in 2018 — a compound annual growth rate of 15.4%. This growth demonstrates both the importance of the market for standalone DDoS prevention products and how companies are investing in preventing DDoS attacks.

The U.S. government has become so concerned about DDoS attacks that it has developed new regulations for some industries. For instance, the U.S. government worked with the Federal Financial Institutions Examination Council (FFIEC) to create regulations for financial services firms. These regulations were issued in April 2014 and introduced six steps that financial services firms should take to protect themselves and their customers from the effects of DDoS attacks. These steps range from general security protocol and protection such as evaluating risk, monitoring traffic, and preparing an incident response plan to the recommendation of engaging an outside service provider to manage Internet traffic. Because the finance industry is among the most heavily regulated industries, these regulations could signal broader changes in the future.

Currently, the traditional ways to prevent DDoS attacks include on-premises products such as routers, switches, intrusion prevention solutions (IPS), and firewalls that are managed by the company that owns them. Cloud systems are managed services that include a product or services to manage on-premises solutions. Defense in depth is a hybrid option that employs an on-premises solution for smaller attacks and a cloud solution for larger attacks. Then there are true hybrid solutions that feature integration between the on-premises solutions and the cloud solutions.

Another option is using CDNs to defend against DDoS attacks at the traffic level, approving traffic or not when first allowing it onto a network. This allows protection with edge-based filtering technology. CDNs can also cloak the main server by having all traffic go to the CDN, thus allowing the company to maintain control of its servers and traffic the whole time. The CDN will protect against DDoS attacks at Layers 3, 4, and 7, with most DDoS attacks occurring at Layer 3. Clearly, the CDN is another good option for DDoS defense, and although it has been around a while, it is now being utilized more often.

Definitions

- **Distributed denial-of-service defense:** The DDoS defense market includes products that detect and mitigate distributed denial-of-service or denial-of-service attacks. While DDoS defense features can exist in firewalls, IPS, and other security products, there are also dedicated products targeted at DDoS prevention. These solutions can be on-premises or cloud based — or a hybrid of the two.
- **Distributed denial-of-service attack:** A distributed denial-of-service attack is a targeted attack to overrun the server with traffic, such that the Web site cannot work with all the queries being made of it.
- **Content delivery network:** Content delivery is the process by which content (including static, dynamic whole sites and application programming interfaces [APIs]) created or acquired by a company is delivered over a network to an endpoint for consumption.
- **Application programming interface:** An application programming interface is a cohesive application execution environment for applications built on a server or back-end component.

Key Trends in Attacks and Prevention

As mentioned previously, DDoS attacks are becoming more prevalent as well as more complex. Attackers are able to disguise traffic as coming from legitimate sources instead of from true malicious sources, making it difficult to detect DDoS attacks. Another attacking technique is to have the traffic fluctuating from different attack sources, making it hard to track down the attackers and cut them off to allow the Web site to work normally again. One complexity that's also becoming more prevalent among attackers is layering attack vectors, combining application layer attacks with network layer attacks. Such assaults may combine scripting attacks with millions of clicks per second to the "Add to Cart" button, or they could target a company by inputting random usernames and passwords into a site log-in form continually while also flooding the host ports at the network layer to make the Web site shut down.

New prevention techniques have arisen to combat these new attacks. One such technique involves incorporating DDoS prevention into more products. CDNs provide opportunities to ward off DDoS attacks at the network level and the application level, allowing further protection and preventing combination attacks. Another prevention technique involves using a hybrid approach for DDoS defense by integrating the on-premises device with the cloud scrubbing service. This technique employs the on-premises device to prevent low and slow attacks and the cloud scrubbing service to prevent larger, faster attacks.

Considering Fastly

Fastly is a CDN provider with offices in San Francisco, New York, London, and Tokyo. CDNs help Web sites, mobile applications, and APIs deliver content faster to consumers. Fastly services a stable of well-known retail and media clients, including Boots UK, Conde Nast, Etsy, Hearst, Hotel Tonight, Kayak, Twitter, and Wayfair, as well as enterprise businesses.

The start-up company differentiates its service by offering real-time everything, including analytics, configuration, instant purging, integration with DevOps platforms, and Varnish Configuration Language (VCL) controls. Fastly's API allows for real-time configuring and complete control of the Web site. This real-time technology also allows for real-time analytics and logs, which are beneficial for further understanding what is happening on the Web site and for up-to-the-second control of the content. There is also the ability to have an Origin Shield, where customers can designate a specific point of presence (POP) to serve as a shield for their origin servers. Content is then fetched from the shield server, reducing strain on a customer's origin server. Additionally, Fastly's Varnish open source Web accelerator allows the company to accelerate dynamic content, APIs, and logic at the edge. Fastly has highly customized Varnish to suit its needs and be scalable. Clients can also customize the VCL to define their caching policy by writing code or utilizing Fastly's Web interface that will easily generate a VCL to customers' specifications. Custom security threat detection and filtering can also be coded at the edge using VCL (by Fastly's engineers or the customer, as Fastly provides full capabilities for customers to write their own detection and filtering logic).

Fastly was founded primarily as a CDN provider, but the company's position on the network presents a unique opportunity to provide advanced security to Fastly clients. The company has the ability to create logic that runs at the edge of the network — closer to both the end users and the source of attack traffic. Companies can take advantage of edge authorization or a paywall, Geo IP, mobile device detection, shopper prioritization, and data collection (this is critical for IoT services). In addition, Fastly's place on the network allows for protection against attacks on all levels of the network, giving the company's solution a distinct advantage over other security products.

How Fastly Provides DDoS Protection

Fastly can help protect the edge of the network against Layer 3 and Layer 4 attacks. It also performs at the edge of the cache, allowing Layer 7 protection handled by the VCL. Additionally, there is the ability to filter traffic at the edge of the network and to enhance that filtering functionality by integrating it with third-party threat feeds and the real-time propagation of changes. The solution's real-time logs and statistics provide up-to-the-second visibility and control that allow rules and configurations to be changed as quickly as attackers can alter their attacks.

Since Fastly is not an on-premises solution, it has the capacity to handle an attack of several Tbps, compared with an on-premises solution that can handle only up to a 1Gbps attack. Another benefit of Fastly is the overage protection that allows a large amount of traffic on the network while maintaining a consistent invoice. Fastly is also certified as a Level 1 service provider compliant with the Payment Card Industry (PCI) Data Security Standard.

Challenges

The main challenge for Fastly is that its clients may not be aware of all the company has to offer by way of security functionality. This functionality also may appear to be another layer of protection to companies as opposed to a way to prevent DDoS attacks. While it may provide a competitive edge when someone is purchasing a CDN, if the security team at the client does not speak with the networking team and integrates this functionality into the security posture, then it is a feature that won't be fully utilized.

Furthermore, these DDoS abilities may be underutilized because a company has a specific budget to handle DDoS attacks. Poor communication between departments could prevent any of the funds from being allocated to the CDN, or this advantage may be passed over entirely because it is not a dedicated product. To maintain its edge, Fastly also needs to show its product can comply with all the government regulations. Additionally, as DDoS attacks become more complex, Fastly will need to continue to focus more heavily on security and make it a core function of its business.

Conclusion

Fastly provides a unique view and ability to defend against DDoS attacks. Its view into the data is real time, and being able to reconfigure the network in real time provides an advantage that would not otherwise exist — the attack defenses can be as agile as the attackers. There is also an origin cloaking feature available through Fastly that hides the customer's origin servers from anyone but Fastly's network. A common method attackers will revert to when an application is behind a CDN is to direct the attack traffic at the origin server, bypassing the CDN protections. The Fastly offering hides the origin completely from the attackers, forcing all attack traffic through the CDN.

To help deal with some of the challenges described, Fastly could work with both the networking team and the security team at the time of purchase to make sure both departments at the company understand the solution's full capabilities and advantages. Additionally, Fastly could verify that its solution would be compliant with the new government regulations. Furthermore, by continuing to show dedication to its DDoS abilities, the company can demonstrate that it can be the main DDoS defense and will change as the attacks do. This approach will allow Fastly to flourish as both a CDN provider and a security solution.
