Protect Against Evolving DDoS Threats: The Case for Hybrid

CIOs want harmony. Security directors loathe point products. Network operations won't buy into anything new. CIOs can get the harmony they need around DDoS mitigation by extending the F5 Application Delivery Controller into a hybrid solution: on-premises with a new cloud component.

White Paper

Introduction

DDoS attacks are constantly changing. While the objective of the attack is still to cause a service outage, attacks and attackers are becoming more sophisticated. The motivation behind the attacks is increasingly financial or political—with more serious consequences for the targeted victims. High-profile organizations, such as financial institutions, governments, and service providers, continue to be targets. But a rising number of everyday businesses also report DDoS attacks. The escalating incidence and severity of these attacks has made DDoS expertise a high priority for many a CIO when searching LinkedIn profiles. The problem CIOs face now is how to choose a solution.

Meanwhile, on-premises DDoS solutions have been unable to expand outside their point products to deliver any value beyond mitigation. To this day, if they aren't being used for a DDoS attack, they are just drawing power, subtracting budget, and adding latency.

Service providers are in the right place at the right time with a narrow scope of volumetric protection, typically at a low cost. But anecdotal reports from many customers suggest that with regard to quality, the adage applies: You get what you pay for.

Media frenzy around DDoS has also brought many vendors into the market, but with mixed results. The efforts of content delivery networks (CDNs) to extend into the market have largely fallen flat. Other cloud solutions have mismanaged themselves into isolation and obscurity by acquisition.

What Every CIO Really Wants

CIOs and their security directors want confidence in their DDoS mitigation system. To achieve this, they need a solution with the following properties:

- Defend: Must have a cloud component for volumetric attacks.
- Block: Must be able to block application DDoS without requiring SSL key surrender.
- Deploy: Must be acceptable to the network operations team.

The CIOs and the security directors are tired of point products. For example, security directors have reported that while their organizations have purchased as many as 200 different point products for security and analysis, it's not uncommon for operations teams to install only a few. The rest remain shelfware.

Many CIOs have been unable to turn to the cloud for their application security needs because of a critical factor—SSL. As more and more applications become protected with SSL, cloud solutions are prevented from monitoring and mitigating application-level attacks such as GET floods. An on-premises solution is required for SSL and a cloud component is required for volumetric attacks.

The Right Way to Protect Against DDoS Attacks

F5 has championed a unique on-premises value proposition. By integrating a network firewall into the Application Delivery Controller (ADC) and combining SSL termination with OWASP Top-Ten mitigation at a second tier, F5 has met two of three critical needs. And with F5® Silverline™ DDoS Protection—a service delivered via the F5 Silverline cloud-based platform—F5 now has the final piece of the puzzle that gives the CIOs exactly what they're looking for.

F5's unique, hybrid DDoS mitigation solution protects against volumetric attacks from the cloud, handles application level attacks on premises, and is instantly acceptable to network operations teams, many of which already trust F5.

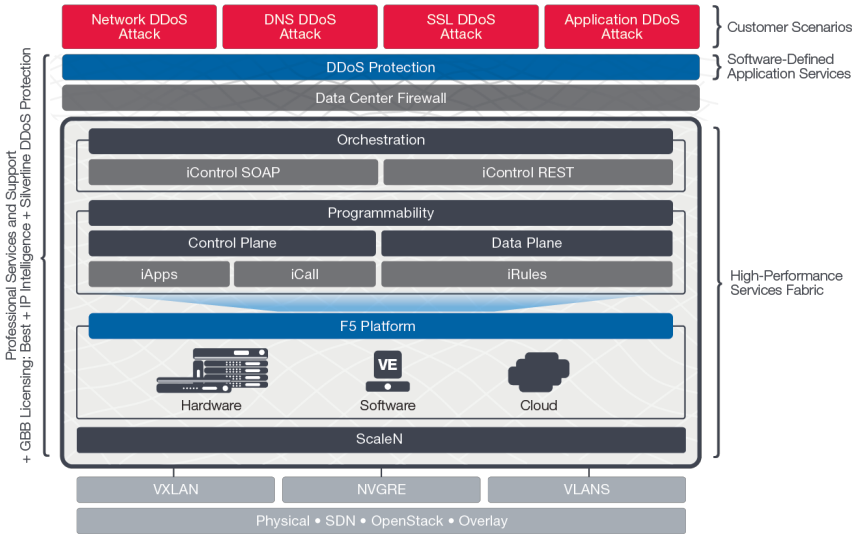

Figure 1: A comprehensive DDoS solution includes both cloud and on-premises components.

CIOs Should Get What They Want

Why the CIO Needs On-Premises DDoS Protection

When F5 first provided DDoS protection in 2001, the attacks were crude, with many SYN floods and simple network-level attack vectors. Attackers have since become more sophisticated, with multiple methods for bringing down a host (or network) or clogging an ingress (or even an egress) pipe.

The most common attack today is the customized GET flood. In this attack, the perpetrator will spider the target website to find all the expensive database queries and large PDF files that might litter the brochureware section of the marketing site on the server. With this list in hand, the attacker will then repeatedly request these resources.

It can be difficult to distinguish between malevolent and legitimate requests for data. Increasingly, these requests are delivered via SSL-encrypted connections. The encryption prevents cloud solutions from being used to mitigate or even analyze the problems.

CIOs need on-premises protection that can decrypt the traffic, see the aggregate of the malicious requests, and then attempt to mitigate. The F5 solution inserts itself into the traffic, making the analysis and then injecting challenges into the steam itself. Security teams have leveraged the programmability of the F5 platform to do exactly this kind of work for years.

Why the CIO Needs Cloud

Recently, three different types of so-called amplification attacks were used to cast enormous storms of volumetric traffic.

In 2013, the DNS infrastructure was weaponized during an attack against the Spamhaus project. The attack leveraged over 20 million misconfigured DNS servers. The Open Resolver Project handily provides a list of the servers, which are basically a public botnet for anyone smart enough to figure out how to forge spoofed DNS requests. Despite some early publicity, the number of open resolvers is actually continuing to grow at an alarming rate. Given the effectiveness of these DNS amplification attacks, it's a wonder that we're not seeing these open servers in attacks used more often.

Just a few months after the Spamhaus event, another Internet protocol was found to be susceptible to mass manipulation. This time it was the dated Network Time Protocol (NTP). An administrative door had been left open that allowed anyone to request that the NTP server reply with a list of the previous 600 clients. The source of the request was never validated, so thousands of NTP servers could easily be asked to blast a target with millions of responses, quickly filling the target's ingress avenue. On February 11, 2014, the DERP Trolling group used this technique to attack the gaming servers being used by a gaming rival.

Finally, attackers have been abusing the clunky SNMP protocol. In one case documented by the SANS institute, video conferencing systems amplified SNMP "GetBulk" requests to attack with a multiplier of nearly 700 times. This led SANS to suggest that the attack may be a showcase for a whole new Internet category: the "Internet of DDoS Things."

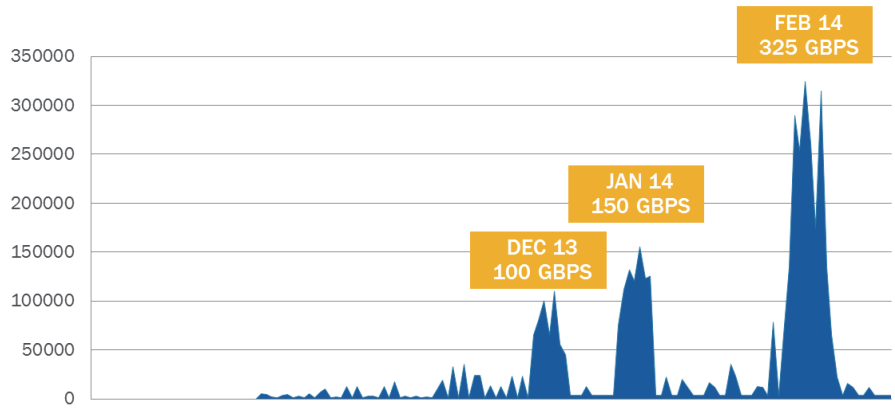

Figure 2: 2014 volumetric attack trend.

The trend shows that attackers keep inventing ways to turn the Internet against itself. The sizes of their peak volumetric attacks continue to grow. No amount of JavaScript challenges or rate-limiting is going to deal with all the traffic on premises. A cloud solution with terabits of capacity is the only solution for these attacks.

These types of volumetric attacks are exactly what F5 Silverline DDoS Protection is designed to defend against. Organizations can use the Silverline DDoS Protection subscription offering, Always Available™, as a primary level of defense, or pass all traffic through SilverLine all the time with the Always On option.

On-Premises and in the Cloud: the Ultimate Solution

CIOs need an on-premises solution that is acceptable to the network operations team. They also need a cloud component to be an insurance policy against hurricane-sized DDoS storms. What would be even better? A hybrid solution where each side is aware of the other.

Until flow-based detection and mitigation standards are in place, CIOs must rely on a vendor solution.

- F5's on-premises component has value beyond mitigating attacks. All other on-premises solutions are specific to DDoS mitigation, whereas the F5 DDoS technology is integrated into components that serve other functions such as network firewall protection or PCI compliance through the web application firewall. This means that the solution is not just a policy; it provides value every day, delivering the business application and protecting it from OWASP Top Ten. A CIO can then leverage the investment in the F5 solution, rather than in a point product, to solve other problems for the organization.
- The acceptance and successful deployment of the solution by the network operations team must be considered. Because F5 is ubiquitous throughout major data centers, it is already an accepted and embraced vendor. In many cases, implementing DDoS solutions for F5 is as simple as activating code that is already resident at the ADCs.
- F5 offers defensive technologies such as SSL tunnels, global load balancing, application monitoring, user authentication, and context tracking. Imagine these technologies working together across the barrier between on-premises and cloud. Or between data centers. Or orchestrating the mitigation of application DDoS attacks among multiple data centers—from a cloud built around the same F5 solutions that exist in each of the data centers.

With its cloud operation centers and professional services, F5 is a veteran in DDoS mitigation. The experience of owning the data center solution and the cloud solution—and understanding trends in both attacks and in the marketplace—makes F5 uniquely positioned to execute on its vision of comprehensive DDoS protection.

Conclusion

CIOs should get what they want—assurance. For DDoS, that assurance will come when these needs are met:

- The data center is able to block network volumetric attacks and application DDoS attacks, ideally without using point products.
- The CIO knows that the chosen solution will be embraced by the operations team.
- The organization has a cloud component for volumetric attacks. The answer to these needs has crystallized into the F5 DDoS Protection solution.

Consider: The on-premises solution provides the value of delivery applications every day of the year. It will also be deployed, since it isn't just another point product and F5 is a trusted vendor. F5's application security protection, which is counterbalancing the OWASP Top Ten, can also provide the application layer DDoS protection. The F5 cloud component provides that final insurance policy against volumetric attacks, too.

Only F5 is putting all of these factors together in a single, unified solution—protecting your organization now and into the future.

F5 Networks, Inc.
401 Elliott Avenue West, Seattle, WA 98119
888-882-4447 www.f5.com

Americas
info@f5.com

Asia-Pacific
apacinfo@f5.com

Europe/Middle-East/Africa
emeainfo@f5.com

Japan
f5j-info@f5.com