IDC TECHNOLOGY SPOTLIGHT

Sponsored by: A10 Networks

Enterprises are seeking new layers of protection from distributed denial-of-service (DDoS) attacks. Service providers, leveraging new approaches to DDoS protection, are in an excellent position to capitalize on changing market expectations and deliver high-value services as a key competitive differentiator.

New Approaches to DDoS Protection Offer Better Security and Economic Scale

June 2019

Written by: Christopher Rodriguez, Research Manager, Cybersecurity Products

Rethinking the Economics of DDoS Defense

Distributed denial-of-service (DDoS) attacks are more vicious than ever, with attack sizes reaching a scale that has jumped by an order of magnitude in as little as five years. For enterprises, the ability to handle DDoS attacks in-house becomes a steeper challenge with each passing year as attackers find new methods to amplify attacks. More pressing still is that the 5G rollout is in its early phases but will arrive soon and will offer attackers tremendous resources with which to generate massive attacks. In light of these new attack trends, DDoS defense architectures must evolve at a faster pace.

AT A GLANCE

KEY STATS

- 41% of companies surveyed by IDC faced DDoS attacks more than 10 times per year; 3% were attacked over 100 times.
- Over 20 million total devices have been found to be exploitable as DDoS reflectors.

Yet, enterprises are increasingly identifying limitations to the DDoS defense options available to them — chiefly, that the cost of DDoS defenses is manageable for large enterprises but presents an overly oppressive expense for smaller organizations. DDoS mitigation appliances are a wise investment for businesses that face a regular, steady stream of attacks but not for business facing infrequent attacks. Cloud services add a sizable overhead cost to online operations, while on-demand cloud services present unpredictable costs.

As a result, enterprises are seeking new layers of protection, leading them to reevaluate their expectations of what level of protection service providers can offer. Service providers, leveraging new approaches to DDoS protection, are in an excellent position to now capitalize on changing market expectations and deliver high-value services as a key competitive differentiator.

Service providers can attract and retain enterprise clients through high-performance security offerings that eliminate the risk of costly and embarrassing DDoS downtime. However, the strategy has faced challenges — scalability, profitability, shortage of trained personnel, and fear of false positives constrain the ability of service providers to deliver enterprise-specific solutions. Interestingly, service providers are finding that the DDoS defenses that worked for their infrastructure protection will not scale to provide the granular controls required for defending enterprise tenants. Service providers must grasp that enterprise needs are different, varying from one customer to another. This paper highlights the shifting dynamics of DDoS defenses and outlines options for service providers to deliver effective, value-adding, and profitable security solutions.

Benefits: Automated and Intelligent DDoS Mitigation Drives Scale and Profit

Modern approaches to DDoS mitigation solutions that scale granular controls and operate autonomously will help service providers evolve beyond their current limitations. This approach addresses the fact that traditional DDoS defenses that worked for their infrastructure protection will not scale to provide the granular controls required for defending enterprise tenants.

Traditional DDoS defense solutions designed for infrastructure protection were originally built to ensure the ability of the operator to deliver data services without interruption from volumetric DDoS attacks. Smaller, sophisticated attacks targeting network and application resources do not impact the service provider's data delivery services, so these types of attacks are ignored and passed through to the subscribers to deal with. When a subscriber is targeted for a menacing volumetric attack, the operator will blackhole the traffic upstream, thereby eliminating the attack but assisting the attacker in knocking the victim offline — effectively sacrificing one to protect many others.

Enterprise DDoS defense requirements are different; enterprises need protection for smaller networks that are application centric. These protection points require individual granular detection per service and DDoS defenses that provide full-spectrum, volumetric network and application layer protection that traditional service provider defenses are unable to deliver.

Service providers seeking to advance their ability to deliver valuable enterprise DDoS defense services should invest in modernized DDoS mitigation solutions that offer large multitenant scaling and automation. These characteristics are the foundation of a security offering that delivers superior value for customers as well as enhanced business results for the provider:

For service providers, the ability to leverage automation and multitenant scaling is tantamount to success.

- Autonomous operation is required to rapidly detect and mitigate multivector threats across complex networks, without resource-draining manual interventions. This helps reduce burden on security operations center (SOC) staff and improves efficacy at large scale.
- Providers must be able to scale DDoS protection services to tens of thousands of business subscribers to protect applications and generate revenue from small, compact form factors.
- Providers need to offer flexible delivery of differentiated levels of protection to meet subscribers' available budgets and acceptable risk, thereby enabling broad subscriber coverage and maximized profits.
- Providers should intelligently differentiate attacker from user traffic to minimize collateral damage against the tenant and meet stringent service-level agreements (SLAs). Reduction in false positives and competitive SLAs can help improve customer satisfaction and retention rates.
- High performance, in terms of both network throughput and connections per second, is required to defend against large-scale attacks without "dropping" customers. This capability becomes more urgent as the Internet of Things (IoT) promises a boom in the number of possible attack devices.

For service providers, the ability to leverage automation and multitenant scaling is tantamount to success. Invariably, after starting a scrubbing service, service providers typically see a spike in observed attacks. The spike is a result of visibility into the more frequently smaller, yet equally devastating, attacks directed at the tenants that were previously

ignored. At these accelerated rates of DDoS occurrences, the manual intervention that was acceptable against infrequent massive volumetric attacks will no longer be viable.

Key Trends: Escalating DDoS Risk Drives Enterprises to Service Provider Partners for Defense

With constant growth in the volume and ferocity of DDoS attacks, enterprises are hard-pressed to handle DDoS risk on their own. For example, the IoT-powered Mirai attacks of 2016 introduced the world to the age of the 1Tbps+ DDoS attack. In 2018, the Memcached attacks used amplification and reflection techniques to achieve the enormous scale of 1.4Tbps of attack traffic; later that year, another DDoS attack peaked at 1.7Tbps. Smaller, but still devastating, DDoS attacks in the 100Gbps+ range have increased as well. The rollout of 5G will present massive bandwidth and numbers of IoT-connected devices to exploit. For example, in late 2018 researchers discovered that over 400,000 IoT devices were exploitable as CoAP DDoS reflectors—the CoAP protocol can be abused to amplify DDoS attacks by a rate of up to 35x. In total, researchers have identified over 20 million devices that are vulnerable to abuse as DDoS reflectors, via CoAP and other protocols.

Enterprises must invest in a DDoS mitigation product or service that best meets their needs for balancing risk and security against cost and, in particular, the high costs associated with always-on cloud scrubbing services. Yet, enterprises are attacked on a regular but unpredictable basis. According to IDC's 2018 U.S. DDoS Prevention Survey, 41% of respondents were attacked more than 10 times per year and 3% of respondents were attacked over 100 times.1 The unpredictable nature of DDoS attacks causes enterprises to prioritize common and consistent attack vectors such as endpoint malware, email, and web, as well as unpredictable but potentially catastrophic threats such as advanced persistent threats (APTs), advanced malware, and fileless attacks.

As a result, many enterprises are outsourcing protection, in part or in total. Service providers have an opportunity to play an important role in the next generation of DDoS defense strategies. Service providers are naturally in the path of traffic flow and so are well positioned to handle the DDoS attack upstream, before the attack reaches critical mass. This positioning offers the advantage of intercepting the attack traffic in the native path, compared with the cloud scrubber's need to divert traffic to other internet-connected centers for scrubbing, which adds latency, complexity, and the potential for private data exposure.

Overall, the growing sentiment is an expectation that service providers must be more than packet movers — if customers pay for internet service, then it should also be available, regardless of attacker activity. Rather than a burden, this change in customer expectations presents a useful opportunity for service providers to deliver more value to customers and achieve differentiation from the competition. By effectively executing managed scrubbing services programs, service providers are in an advantageous position to compete and win in the lucrative DDoS mitigation market.

Considering A10 Networks

A10 Networks entered the DDoS defense market in 2014, rapidly building out a comprehensive DDoS mitigation portfolio of solutions for enterprises and service providers alike. A10 Networks DDoS protection solutions have been adopted by large organizations spanning many industries, including some of the largest cloud providers as well as gaming, financial, and mobile operators and hosting providers worldwide. A10 Networks has adopted a market strategy that focuses

[1] *DDoS Protection Is Now a Necessity and Still Growing: U.S. DDoS Prevention Survey* (IDC #US43904418, June 2018)

heavily on security efficacy, intelligence, and automation, with a goal of solving the scale and performance issues required for defending against tomorrow's attacks.

A10 Networks provides a complete set of surgical DDoS defense capabilities using comprehensive multivector application and network attack defenses. This is augmented by an included threat intelligence feed, powered by the A10 threat research team and 50+ other sources, to ensure known bad actors are blocked according to established policies, with regular updates to ensure accuracy. Policies are uniquely escalated through increasingly more rigorous defenses as attacks escalate. This approach ensures high security efficacy but also avoids collateral damage.

A10 Networks also innovatively leverages its full portfolio of security solutions to deliver distributed detection, called One-DDoS. A10 Networks' CGN, CFW, and ADC products act as detectors throughout the network, using full packet-based data to detect attacks directly from the targeted services. Detection costs are reduced because fewer dedicated DDoS detectors are required. This approach offers the benefit of packet-based detection versus sampling improves response time and the quality of data analyzed to make protection decisions.

Most recently, A10 Networks introduced additional new automation capabilities that improve security effectiveness and simplify operation with its Zero-Day Automated Protection (ZAP). A10 Networks' ZAP helps service providers overcome DDoS defender and scrubbing service staffing shortages. In addition, it helps increase the speed of response by applying artificial intelligence (AI) via machine learning (ML) and heuristics-based expert systems that identify the attack strategy and calculate the required blocking filters in real time with no manual intervention or previously staged configuration.

A10 Networks' DDoS products have been well known in the industry for high-end performance. The company offers software VNF versions starting at 1Gbps, and Thunder hardware appliances can provide up to 500Gbps of blocking protection in 1RU form factor. For enterprises, a hybrid solution combining a prepared service provider with on-premises hardware or software and cloud scrubbing is generally preferred.

Traditionally, service providers have been hampered in their ability to offer enterprise-specific DDoS protections at scale. A10 Networks addresses these limitations with the following solution components:

- **Zero-touch operation.** A10 Networks' fully automated DDoS defense capabilities include an automated five-level adaptive policy, ML-powered zero-day attack protection, and actionable threat intelligence covering DDoS weapons.
- **Multitenancy.** A10 Networks supports multiple tenants with granular policies and different tiers of service (e.g., 256,000 individual detection profiles per appliance and 3,000 active mitigations per appliance). This gives scrubbing service operators the ability to support tens of thousands of business tenants with individual detection and mitigation policies from a single defense platform.
- **Analytics.** A10 Networks uses machine learning to enable automation such as continuous learning user baseline and Zero-Day Automated Protection.
- **Low impact.** Flexible deployment modes with multimodal source tracking defenses help minimize false positives and user impact.

- **Service provider–specific features.** A10 Networks offers solutions for protection of critical service provider services such as CGNAT, DNS, and SIP and can leverage these solutions as additional DDoS detection points. All A10 Networks solutions are SecOps and DevOps ready with 100% RESTful APIs.

Case Study

Achieving effective automated defense allows service providers to deliver value-adding services that yield profits and additional business benefits. For example, a global web-hosting provider shared its experience of offering two tiers of DDoS defense for subscribers: basic for all subscribers and advanced as a premium service. The company reported:

- Service-generated profits
- Increased net promoter scores
- 11% drop in filed support tickets

Challenges

In recent years, A10 Networks has emerged as a strong competitor in a well-established market, but it must compete against vendors that have over a decade of history in DDoS protection. Highly visible key competitive wins and the ongoing development of differentiated innovative new features will help A10 Networks continue to advance.

Additionally, with the rollout of 5G now starting in earnest, service providers have extensive investments to make in new infrastructure. For service providers, the need to deliver new revenue-driving services is balanced by the need for cautious investment. Successful rollouts of advanced DDoS mitigation services by innovative service providers will further demonstrate the benefits of A10 Networks' intelligent and automated DDoS detection and mitigation solutions.

Conclusion

The DDoS mitigation market is evolving rapidly as service providers identify new expectations and opportunities to deliver high-value DDoS mitigation services to subscribers. A10 Networks offers advanced automated DDoS detection and mitigation solutions, capable of high scale, while frequently innovating new capabilities that are required for communications service providers to serve their customers and enterprises to survive the next generation of threats. Such scalable new options may prove to be the difference in tilting the economics of DDoS defense back in favor of the good guys.

About the analyst:

Christopher Rodriguez, *Research Manager, Cybersecurity Products*

Chris Rodriguez is a Research Manager in IDC's Cybersecurity product research group focused on the products designed to secure today's complex enterprise networks. IDC's cybersecurity research offerings to which Chris contributes include Endpoint Security; Network Security Products and Strategies; Security Analytics, Intelligence, Response, and Orchestration (Security AIRO); and Identity and Access Management research programs.

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com