Service Provider Requirements for DDoS Mitigation:

Protecting Networks While Improving Optimization and Efficiency

FROST & SULLIVAN

An Executive Brief Sponsored by Allot Communications

Chris Rodriguez

Senior Industry Analyst – Information & Network Security

May 2017

INTRODUCTION

DDoS continues to blight the Internet and hamper every new technological advance, including world-changing trends such as the Internet-of-Things (IoT). Attackers continually discover new methods for generating large volume and sophisticated attacks. The availability of simplified attack tools, DDoS for-rent services, and for-hire attackers has also helped drive the number of would-be attackers, and correlates with a steady increase in the number of DDoS attacks reported each year.

“Service providers find themselves either in the cross-hairs or in the cross-fire—neither situation is optimal, and both are always costly.”

Service providers find themselves either in the cross-hairs or in the cross-fire—neither situation is optimal, and both are always costly. As a result, service providers must update their defenses to meet the challenges posed by evolving DDoS threats, both the obvious and the less apparent. Service providers require solutions that can address challenges that are unique to their networks, and with the potential to yield benefits beyond attack mitigation.

DDOS RISK ESCALATES

DDoS attacks are more formidable than ever, growing year-over-year in terms of scale, frequency, and sophistication. As a result, mitigation of DDoS attacks is now a top priority for enterprises and service providers alike.

DDoS Attacks Achieve New Heights

DDoS attacks grew in volume at a linear rate until 2015, before taking a monumental leap forward in 2016. Peak attack sizes are now reaching the 1 Tbps mark, signaling an entry into a new era of massive volumetric attacks. The largest observed DDoS attacks per year are shown in Figure 1.

Figure 1: DDoS Peak Attack Volumes per Year

Year	Attack volume (Gbps)	Campaign
2012	65	Operation Ababil
2013	300	Targeting Spamhaus
2014	400	Reported by CloudFlare
2015	500	*Organization undisclosed
2016	800 – 1,200	Targeting Dyn / OVH

Source: Frost & Sullivan

The largest attacks are often directed at service providers and network carriers, in an effort to disrupt the victim as well as a multitude of secondary targets. While only a select few service providers face the largest volumetric DDoS attacks, ranging in the 100+ Gbps range, attacks in the 1 Gbps and 10 Gbps range are common, and are an unwanted strain on even the most robust networks. Service providers also experience the effects of attacks on their enterprise customers; the impact of concurrent DDoS attacks against multiple enterprise customers can saturate operator network resources, degrading network service or shutting down the network completely.

DDoS Has Become a Regular Occurrence

DDoS attacks are increasing in frequency each year, often targeting service provider networks. This is partially the result of publicly available attack tools and for-hire DDoS services. Now, anybody can attack an online organization for even the most trivial reason. Service providers can no longer afford to wonder "what if?"; and should be asking "when?" as they consider the possibility of a DDoS attack.

Service providers feel the pain of each of these attacks in some form or another. Attackers may choose to attack a target directly or by targeting service providers as a proxy. Service providers may experience unpredictable network congestion or diminished service availability due to blacklisting by other service providers. Of course, other customers of the same service provider may experience ill effects as a form of collateral damage. This can be problematic for service providers' service level agreements (SLAs) that specify a minimum quality of experience (QoE).

Additionally, business relationships between service providers and enterprises have grown much closer as many offer cloud IT infrastructure services or managed security services. Service providers cannot afford to pass the burden of stopping DDoS attacks to their customers.

Attackers Continually Adjust Their Strategy

Threat actors continue to develop (and in some cases, commercialize) new techniques, tactics, and procedures to aid in their efforts to disrupt and harass online organizations. Prior to 2016, amplification and reflection techniques were the tactic of choice employed by hackers to create the chart-topping DDoS attacks shown in Figure 1. Attackers then adjusted their strategies to find and exploit vulnerabilities in IoT devices, as evidenced by the Mirai-based botnet attacks against OVH and Dyn. Both amplification and reflection and IoT DDoS tactics were used in record-breaking volumetric attacks from 2013 to 2016.

Additionally, attackers modify their own behaviors to evade defenses as well. For example, traditional DDoS detection tools that rely on baselines and sampling require time to accurately diagnose an attack in progress before starting the mitigation process. Attackers now utilize "hit-and-run" style attacks, lasting only a few minutes, in order to defeat time-dependent defenses such as centralized scrubbing centers or on-demand cloud services.

SERVICE PROVIDERS FACE UNIQUE RISKS

As service providers must protect their networks, they also face requirements and challenges beyond what enterprises face. The following are important considerations for any service provider considering a DDoS mitigation solution.

Service Providers are Targets or Targets-by-Association

Service providers may be targeted if they support a business or other online organization that has drawn the ire of cyber miscreants. If an attacker cannot disable its target's website, it may attempt to disable the service provider's infrastructure instead, to undermine the availability or responsiveness of the targeted website. Or a threat actor may focus its efforts on a service provider network from the outset, in the hope of disrupting many enterprise customers at once.

Service providers may also be targeted by threat actors that are simply trying to demonstrate their prowess or test their own capabilities. For these actors, a massive, high-capacity service provider network presents a compelling challenge; while the highly publicized media coverage of a successful DDoS attack represents an enticing trophy.

DDoS Attacks May also Come from Within

In 2016, IoT devices emerged as a new and effective threat vector for DDoS attacks. Yet, a strategy to barricade network entry points from all external IoT devices is insufficient. Service providers report that this method fails when devices within their own network are compromised and turned against the service provider's own resources. Moreover, compromised devices, IoT and otherwise, may be used in DDoS attacks against other service providers, causing the service provider's network to be blocked or limited by peering partners.

> “
>
> A strategy to barricade network entry points from all external IoT devices is insufficient. Service providers report that this method fails when devices within their own network are compromised and turned against the service provider's own resources.
>
> ”

Other Conditions Can Threaten Network Performance or Availability

The goal of a DDoS attack is to consume network resources (including any service provider/IT infrastructure such as firewalls, core network routers, DNS servers, or back-end systems) to the point that they have no capacity left for legitimate traffic. This same situation may occur on a service provider network even if the provider is not under attack, due to either accidental or unexpected conditions.

Accidental Denial of Service

Network congestion is undesirable regardless of the cause. Congestion resulting from a DDoS attack has a definite cause, and must be detected and mitigated immediately. However, network congestion may also have less obvious causes and unintentional effects.

For example, IoT devices do not require either human-to-human or human-to-computer interaction to function. As the number of IoT devices climbs, the amount of cross-talk between these devices is also increasing. This characteristic holds the potential for accidental over-consumption of network resources in the case of malfunction. Such an occurrence may be unpredictable, but service providers must be prepared to respond to such challenges should they arise.

Incidental Denial of Service

DDoS attackers typically rely on utilizing stolen resources, such as malware-infected personal computers, or by abusing servers that are otherwise functioning properly. These compromised or abused devices inevitably access the Internet via a service provider's network. This situation has two incidental and pernicious effects to the service provider:

- The service provider's network may experience congestion from any device, including IoT devices participating in the DDoS attack, even if the attack target is external to the service provider's network.
- If used as part of a DDoS attack against other organizations, the service provider's network may end up on a security vendor's blacklist of automatically blocked IP addresses.

Blended Multi-Stage Cyber Attacks Target Service Provider Defenses

Since 2010, nation-states and criminal organizations have leveraged cyber attacks to achieve their goals. While a DDoS attack is generally considered an availability issue, the reality is that a DDoS attack is just one of the many tools in the arsenals of advanced threat actors. A DDoS attack can be a vital first step in a cyber attack campaign, by overwhelming and disabling network defenses offered by the service provider (such as firewalls or intrusion prevention systems). Attackers could then establish a foothold in the victim's network by installing a backdoor in a backend system, for future illicit activities.

REQUIREMENTS FOR SERVICE PROVIDER DDOS MITIGATION SOLUTIONS

DDoS attacks continue to evolve, to capitalize on new technology trends or to evade known defenses. Accordingly, service providers must revisit their DDoS defenses and strategies on a regular basis, and re-evaluate their effectiveness and ability to meet their needs.

Massive Attacks Will Require Scalability and Efficiency

Massive scale DDoS attacks are the new normal, and this new normal will only worsen as greater numbers of unsecured IoT devices come online. A proactive defensive posture is an important foundation for service providers that face massive scale DDoS attacks. Service providers should begin by setting limiting policies on network infrastructure elements to ensure that they are not overwhelmed. These valuable resources must continue to function to ensure that the entire network or critical defenses do not fail.

Traditionally, service providers have relied on large-scale, purpose-built cloud or centralized scrubbing centers to mitigate large-scale DDoS attacks. While effective, there are two inherent consequences with this approach. First, network infrastructure resources are consumed in backhauling traffic to a scrubbing center, and in returning the clean traffic to the intended destination. Second, all Internet traffic is backhauled to the scrubbing center. Although this approach reduces the volume of attack traffic that reaches the targeted website, network latency is added to the legitimate traffic; and, if significant, this latency could adversely impact the experience of legitimate end users.

Instead, service providers may be better served by high performance DDoS mitigation appliances with sufficient scalability to eliminate attacks, inline and in real-time, at the network edge; far from CSP customers' networks, and closer to the point of attack origination.

Instead, service providers may be better served by high performance DDoS mitigation appliances with sufficient scalability to eliminate attacks, inline and in real-time, at the network edge; far from CSP customers' networks, and closer to the point of attack origination. Dropping attack traffic at network boundaries reduces the burden on downstream routers, and is therefore a more efficient use of network resources. Additionally, the inline mitigation method ensures minimal latency by avoiding the need to reroute customer traffic, and saves on infrastructure costs—a particularly valuable option for service providers that resort to building dedicated scrubbing centers.

Short-Lived Attacks Require Rapid Detection and Response

Passive, out-of-band DDoS mitigation solutions may require several minutes to identify attacks, and initiate the BGP routing required to perform mitigation in a dedicated cloud scrubbing center. Attackers have learned to recognize and exploit this window of opportunity with bursts of short duration attacks.

By comparison, an inline solution is able to detect and mitigate attacks in seconds "on the spot." This method provides more accurate and rapid mitigation of DDoS attacks, including short duration attacks.

When inline DDoS protection is complemented by inline DPI that performs traffic shaping and application prioritization, CSPs also gain the ability to control and maintain QoE for essential traffic, even during an attack. Furthermore, inline DPI-based solutions enable CSPs to identify "normal" traffic behavior, and automatically trigger corrective measures when behavior approaches or exceeds thresholds.

When inline DDoS protection is complemented by inline DPI that performs traffic shaping and application prioritization, CSPs also gain the ability to control and maintain QoE for essential traffic, even during an attack. Furthermore, inline DPI-based solutions enable CSPs to identify "normal" traffic behavior, and automatically trigger corrective measures when behavior approaches or exceeds thresholds. This capability goes a long way towards preventing outbound IoT-based DDoS attacks, or even IoT malfunctions. Inline DDoS protection and inline DPI, working in unison, is a powerful combination to keep networks up and running and performing.

Large Networks Require Broad Visibility

Service provider networks are complex and may have special requirements, such as the ability to support asymmetric routing to enable requests to enter from one peering point, and responses to exit via another. An optimal service provider DDoS mitigation solution would have broad visibility of the network, using multiple inline detection appliances at peering points. A centralized controller would coordinate these inline devices, thereby allowing the service provider to detect attacks that are spread over multiple peering points. This distributed but centrally managed model provides a comprehensive understanding of all network traffic (both ingress and egress), which is required to rapidly detect attacks.

Visibility is also expressed in terms of threat intelligence, and should include metrics that allow service providers to understand their risks better and plan for future attacks. Intelligence combined with network visibility and analytics enables service providers to understand who attacked whom, how, and the impact to the network.

Service Provider Networks Have Unique Requirements

Service providers no longer have the luxury of assigning IoT devices to networks that are entirely separate from other traffic. Networks that share bandwidth with IoT devices require the ability to distinguish this traffic from other sources. For example, the core network may accept traffic entering from access networks such as remote area networks (RAN), digital subscriber line (DSL) networks, cable networks, or mobile networks. The ability to comprehensively detect and mitigate attacks requires DDoS mitigation appliances that can apply granular controls across network entry points.

APPROPRIATE SOLUTIONS OFFER BENEFITS BEYOND PROTECTION

Given the evolution of attack techniques, modern DDoS mitigation solutions must combine a range of detection and mitigation techniques and controls to be effective. A solution that combines the advantages of an inline appliance and a centrally coordinated DDoS mitigation model provides optimal protection, and supports asymmetric routing, application identification, and session awareness. Such a combination is rare to find in a single, purpose-built appliance, but could offer vital capabilities for protecting service provider networks. Importantly, these technologies also offer value in terms of optimization and cost reduction.

Improve Customer and Partner Experience

Inline DDoS mitigation with dynamic analysis techniques and DPI-based traffic analysis provides a multi-layer defense that is optimal for mitigating attacks; and in particular, massive volume attacks that are capable of disabling the network and services. DPI with application session awareness enables service providers to establish a proactive defense by setting limiting policies for each network infrastructure resource. This ensures that traffic to network elements such as firewalls and routers will not exceed their capacity, and that these devices will continue to operate even under attack conditions.

Additionally, the ability to perform device and application identification, and traffic shaping policies are valuable controls that empower service providers to deliver robust and resilient performance to customers. For example, network resources for mobile or CATV can be prioritized and optimized. Traffic can be prioritized based on factors such as application, user, and device type within the context of network conditions or customer expectations. Service providers can also utilize application identification and traffic shaping to prevent delivery of unwanted traffic, such as P2P traffic, to carrier partners.

> Additionally, the ability to perform device and application identification, and traffic shaping policies are valuable controls that empower service providers to deliver robust and resilient performance to customers.

Optimize the Network

Application identification and session awareness provides service providers with powerful controls over their networks, such as enforcing acceptable use policies and segregating their network, as needed. These tools enable service providers to minimize performance-robbing congestion or blocking of essential traffic (e.g., DNS and routing protocol). For example, service providers could prevent IoT devices from competing with subscribers for bandwidth, by setting congestion thresholds and policies to automate traffic management.

Network optimization has a noteworthy ROI proposition as it could extend the life of existing network architecture, and postpone network upgrades. Additionally, network visibility that is both broad and deep can help service providers to understand network conditions and customer requirements more completely, and use that insight to plan cost-effective upgrades.

Offer New Services

Importantly, strong DDoS capabilities enable service providers to deliver a vital layer of protection by ensuring that firewalls and other critical network defenses and infrastructure cannot be disabled by DDoS attacks. For example, DDoS attacks can disable firewalls during the time required for detection and mitigation, which could be several minutes. An inline solution that combines DPI-based policy control capabilities ensures that the firewall and other security infrastructure are protected and functional at all times. This added layer of protection enables the service provider to offer valuable SLAs and security services to customers and certain types of vertical markets.

> An inline solution that combines DPI-based policy control capabilities ensures that the firewall and other security infrastructure are protected and functional at all times. This added layer of protection enables the service provider to offer valuable SLAs and security services to customers

Avoid Collateral Damage

Blocking attacks inline, as they are detected, allows legitimate traffic to pass through, as opposed to rerouting all network traffic to a scrubbing center. This eliminates the "hop" time associated with redirecting traffic to a scrubbing center, and then back to the customer's network.

No less important, asymmetric inline traffic monitoring provided by inline DPI enables the service provider to analyze both ingress and egress traffic—a critical capability to identify an attack (or other unwanted activities) originating from inside the network. This capability is vital because coordinated, multi-stage DDoS attacks can enter service provider networks via one peering point, and generate responses that traverse others. Service providers can then perform necessary actions to avoid being blacklisted by other network operators, such as blocking IP addresses participating in DDoS attacks.

THE LAST WORD

The DDoS threat landscape is as severe as ever, and attackers are discovering gaps in traditional defenses. Service providers are best served by modern DDoS mitigation solutions that offer advanced protection, a high level of performance, and rapid detection and mitigation times.

Service providers must also ensure that network infrastructure is not disabled during DDoS attacks—a particularly challenging goal during the most massive attacks. A solution that incorporates DPI-based techniques with application session awareness/traffic shaping enables the proactive creation and real-time enforcement of policies limiting traffic to critical network infrastructure elements. Protecting these devices from excessive traffic ensures that essential traffic is prioritized and flows uninterrupted, keeping the network and services available at all times.

Solutions that are deployed inline, but that are centrally coordinated, combining dynamic DDoS detection and mitigation measures with DPI-based policy controls, meet these requirements and should have a more prominent position in service providers' DDoS mitigation plans going forward.

Additionally, an investment in an edge-deployed DDoS mitigation solution may also provide added benefits of reduced operational expenses and improved network performance. In such a case, service providers may wish to advance any plans to update their DDoS defenses to an earlier date to reap these benefits.

Lastly, enterprise organizations are already challenged to solve the DDoS problem on their own. Service providers have their own networks to defend, but can also utilize DDoS mitigation services to gain a competitive edge over the competition, offering DDoS mitigation to their own customers as a value-adding feature or as a dedicated premium service.

Chris Rodriguez

Senior Industry Analyst – Information & Network Security
Frost & Sullivan
Chris.Rodriguez@Frost.com

Silicon Valley
3211 Scott Blvd
Santa Clara CA, 95054
Tel: 650.475.4500
Fax: 650.475.1571

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 FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? Contact Us: Start the Discussion

For information regarding permission, write:

Frost & Sullivan
3211 Scott Blvd
Santa Clara CA 95054

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Detroit
Dubai
Frankfurt
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mumbai
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Sarasota
Seoul
Shanghai
Shenzhen
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw
Washington, DC