TECHNOLOGY SPOTLIGHT

DDoS Protection Requires a Refresh

April 2018

Adapted from *Worldwide DDoS Prevention Products and Services Forecast, 2017–2021*, by Martha Vazquez, Christina Richmond, and Rob Ayoub, IDC #US41659116

Sponsored by A10 Networks

This paper examines the changing DDoS landscape. Many organizations have aging DDoS protection devices as part of their infrastructure. Today's advanced attackers are utilizing a host of advanced attack methods that require defenses greared to utilitize a host of protection techniques in order to defend against attacks. The first DDoS attack to reach over 1 Tbps by leveraging IoT devices happened not long ago. Using IoT devices allowed attackers to demonstrate the dangerous potential of devices that were open to the Internet but not well maintained. IDC believes these kinds of attacks will continue as well as attacks that leverage other vectors in order to disrupt business critical services.

Introduction

The DDoS Landscape has changed significantly in the last 3 years. Beginning with Spamhaus and following on from the current IoT threat have heralded in a new era of attacks and a need for new defenses. Organizations can no longer rely on DDoS protection designed to stop a single attack vector. Defenses must be layered and protect the organization from both internal and external attacks as well as attacks against the infrastructure and individual applications.

One of the most notable large attacks in 2016 was the attack on popular journalist Brian Krebs' website, which marked the beginning of the colossal IoT threat. The attack reached over 620Gbps, and the DDoS defense provider was ultimately forced to part ways with its client because of the massive cost. This new Mirai malware turned IoT devices such as video cameras and DVRs into zombie slaves that fueled the botnet traffic of very large DDoS attacks. Not only were some attacks in 2016 massive in size, but many others leveraged short multivector attacks used to cause a diversion against another real threat (typically ransomware but potentially a diversion from network exploitation or data exfiltration). Because of the effectiveness of DDoS attacks, vendors saw an increased interest in DDoS solutions.

The motives for DDoS attacks continue to vary, and industry research shows they may be motivated by malice, political reasons, financial gain, or the theft of intellectual property. 2018 continues to prove that any organization regardless of size, location, or vertical is a potential victim of a DDoS attack. Thus, the DDoS market will continue to require solutions that are dynamic and evolving and are able to address attacks that are frequent, large in volume, sophisticated, and variable, using volume and application flaws to overwhelm targets.

In the past, DDoS attacks were typically full-on floods of malicious communications that overwhelmed a network, causing outages, loss of business, and expensive mitigation. But today, the increased number of IoT devices with inherent weaknesses and the introduction of the Mirai botnet source code

and the Mirai derivatives like Reaper and Satori has fueled the attack surface, causing organizations to look for modern DDoS solutions.

Challenges Faced By Most Organizations

Unfortunately, most organizations simply do not have the resources necessary to address the increasing volume of DDoS attacks. A recent IDC survey showed that nearly 30% of respondents had seen between 6-10 DDoS attacks last year and over 10% had seen 51-100 attacks. Besides the frequency of attacks there are several key challenges that organizations have when facing the modern DDoS threat.

One of the most severe threats to organizations as they suffer DDoS attacks is their inability to control and precisely limit the damage a potential attack can cause. DDoS attacks are designed to overwhelm services and obfuscate whether traffic is legitimate. New attacks are designed to slow/limit services without setting off alarms. Attackers can now take down an organization without the organization even being aware that they under attack

Another threat to organizations is the inability to scale their defences to the new attacks in the wild. DoS attacks are nothing new, but the new threat is the breath/width/geo-diverse expansion of attacks. Related to DDoS, DoS is the problem, but distributed is the weapon.

Similar to other areas of security, there is a skills gap in the area of Cybersecurity in general, which effects the ability of organizations to defend against DDoS attacks. Due to the technical nature of modern DDoS attacks and the difficulty of demonstrating ROI for DDoS protection (since it is an attack that “could” happen) many organizations struggle with dedicated and appropriate amount of resources to defend against attacks.

As alluded to in the previous challenge, DDoS attacks are not a certainty (although most organizations report experiencing them annually) and it is difficult for organizations to determine how much budget to allocate to defend against attacks. As the industry has seen recently, very large attacks are starting to become more frequent and it may be more cost effective for users to have a short term, on-demand solution in place as opposed to trying to protect against very large attacks 24x7.

In the same survey mentioned above, 63% of respondents said they saw attacks last between 0-10 hours and another 23% of respondents saw attacks lasting 11-24 hours. Those time amounts are enough to cause significant financial impact to an organization or worse if the organization provided life-saving services (such as hospitals)

Benefits

While many customers recognize the need for a dedicated DDoS solution, there are many customers who are still relying on outdated, volumetric focused protection. Given the increasing attack trends towards more sophisticated application and multi-vector attacks, there are many customers likely to be ill prepared for the DDoS attacks that IDC predicts are set to not only continue, but grow in scale and complexity.

At the end of the day, organizations can gain a variety of efficiencies by moving to modern DDoS solutions. A modern solution can allow an organization to successfully address a wide breadth and size of different attacks and stop attacks without risking impact to the rest of the business. The more precisely that a solution can stop a specific attack – beyond just dumping traffic to a null IP address – will enable the business to continue operations. Many attacks are designed to fool traditional DDoS defenses by emulating legitimate traffic. Modern solutions are smart enough to differentiate attack

traffic from legitimate, high-volume traffic to a site and take appropriate actions that do not punish legitimate users.

Another key strength of many modern DDoS solutions is their ability to leverage Threat Intelligence to better address specific attacks. DDoS differs from security threats like ransomware or phishing, where the attacker uses sleuth technics to create a needle in a haystack. Whereas in DDoS, the weapons are the haystack. Threat researchers add a much-needed analysis to the noise, helping to filter out attack traffic from legitimate traffic and looking for clues left behind by specific attackers. This information can then be fed into solutions to proactively stop attacks before damage mounts.

Finally, modern solutions can use automated responses to improve remediation times and to lower overall costs. As machine learning and artificial intelligence (AI) finds it way into modern solutions, those solutions can be smarter, making automated decisions much faster than human analysts.

Trends

This paper discusses the shift in the attack landscape, but there are additional trends occurring in the industry that customers should be aware of as they look to futureproof their organizations against DDoS attacks.

Innovative Technology Fuels the Attack Surface

Digital transformation(DX) is top of mind for many organizations, drastically changing how organizations operate, deliver services, and such. IoT is just one of the accelerators driving this change. However, security is usually added on later in the deployment process. The Mirai and its derivative botnets illustrates the ease with which DDoS attacks can attack IoT devices, leading to the worsening of problems. In addition, the increasing reliance on digital systems intensifies the impact of DDoS attacks.

Readily Available Attack Tools

Acquiring DoS and DDoS attack tools is as easy as searching for them online, selecting one or more, and downloading them. Further, entrepreneurial adversaries are continually developing new methods of attack and making them available in places like the dark net. Any organization is susceptible to these attacks because a DDoS attack can be launched for as low as $19.99. It is even becoming common to see reports of students launching DDoS attacks against their school just to avoid taking a state test.

Considering A10 Networks

A10 Networks offers a modern DDoS solution that can address the wide range of attacks available to attackers today as well as zero-day threats. A10 combines cloud scrubbing along with on-premise protection to give organizations a complete solution against volumetric, network protocol, application, slow and low, multi-vector, and IoT based attacks. A10 Networks offers a wide breath of individual DDoS products that can be combined in order to address attacks on-premise and in scrubbing centers, giving customers the broadest set of coverage against modern attacks.

A10 DDoS Threat Intelligence service provides accurate and timely intelligence that includes millions of known DDoS botnets (e.g., Mirai) and agents used for reflection attacks (e.g. DNS, Memcache, NTP). Thunder TPS supports class-lists that scale up to 96 million entries to make the threat feed actionable and stop DDoS attacks in their tracks.

While threat intelligence provides great insight into attacks, the ability to create an actionable response is key to stopping DDoS attacks quickly, before they interfere with business-critical

functions. By combing its threat intelligence capabilities with intelligent automation, the solution helps simplify deployment, automate wartime operations, and reduce response time.

The Thunder TPS appliance delivers strong performance in a variety of form factors. These appliances are designed to operate in a smaller footprint than many solutions on the market. In fact, today, A10 provides the industry's highest performance appliance with their Thunder 14045 TPS delivering 300Gbps with 440 Mpps in a single 3RU appliance. Many organizations are hesitant to deploy racks upon racks of hardware and many DDoS solutions require just that in order to handle the large attacks that are prevalent today. A10 is mindful of the datacenter and cost requirements of many customers and has designed its DDoS appliances accordingly.

A10 offers cloud scrubbing services that are backed by its purpose-built, globally distributed scrubbing centers, scaled to handle the largest known DDoS volumetric attacks, all orchestrated by A10 DDoS Security Incident Response Team (DSIRT). These scrubbing centers are designed to work in coordination with small, high precision on-premise protection in order to give organizations the most scalable and complete protection possible.

Finally, the A10 solution is future-proof. The solution today is not only IPv6 ready, but actively mitigates attacks against IPv6 protocols and networks. A10 provides full parity of protection mechanisms between IPv6 and IPv4 protocols. Many solutions are better at protecting against IPv4 attacks due to the history with IPv4 but customers are starting to see attacks targeting IPv6 specifically.

Challenges

There are two key challenges that A10 networks will need to address in order to be successful in the DDoS protection market. The first challenge is that the DDoS protection market lacks a consistent response to the problem. DDoS security providers include telcos, pure-play providers, content development network (CDN) providers, security vendors, and managed security providers. There is no standard approach and certainly no single size that fits all requirements. The wide range of providers and pricing coupled with the many varied attack types make it difficult for organizations to determine requirements for a solution, much less budget for one.

As a result, many enterprises rely on on-premises devices such as intrusion prevention systems and firewalls that have built-in defenses, or they are using defense-in-depth solutions, with partial integration or no integration. Or, they may be focused only on volumetric attack protection. Secondly, IT budgets and resources are stretched thin. They have been for some time and will remain so for the foreseeable future. Business leaders have to make tough choices to address issues that are "happening now" versus those that "might happen in the future." They are rationalizing security risks — essentially rolling the dice — and allocating dollars to initiatives they may view as having a higher priority.

IDC believes that A10 is well positioned to address these challenges based on the many factors listed in the above section. By offering a complete solution – cloud and on-premise – along with automated response and a reasonable price tag, A10 has a compelling story to take to organizations that may be confused with the plethora of options facing them today.

Conclusion

IDC believes the DDoS market will continue to be important as organizations continue to move more of their mission critical applications and functions to face externally. Many vendors and organizations are still leaning on dating technology for protection and IDC believes that the scale and complexity of DDoS attacks will continue to increase significantly for the foreseeable future. IDC believes A10

Networks is well positioned to address the challenges described in this paper and the company has a significant opportunity for success globally.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 idc-fi.com