IDC Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Optimizing DDoS Mitigation Using Hybrid Approaches

March 2015

Adapted from *Worldwide DDoS Prevention Products and Services 2013–2017 Forecast* by John Grady, Christina Richmond, Christian A. Christiansen, et al., IDC #239954, and *Worldwide DDoS Prevention Products and Services 2014–2018 Forecast* by John Grady, Christina Richmond, Christian A. Christiansen, IDC #251384

Sponsored by Radware

The prevalence and duration of distributed denial-of-service (DDoS) attacks are on the rise. Organizations, therefore, need to take steps to protect their infrastructure from the advanced methods employed by today's attackers. Despite the fact that volumetric-based attacks will remain the most common, more advanced hybrid attacks that include application layer and encrypted traffic are spurring growth in the use of a hybrid defense solution, which integrates Layer 3 and Layer 7 on-premise detection devices with cloud signaling to mitigate DDoS attacks both in the cloud and on-premise. This represents a newer and more comprehensive approach that a number of organizations are beginning to consider. This IDC Technology Spotlight discusses these trends and considers the role that Radware's hybrid DDoS solution plays in this emerging market.

Introduction

Awareness of the DDoS threat continues to rise in the media, among enterprise security departments, and even in the boardroom. While DDoS attacks began within gaming and gambling Web site businesses, newer attacks have been used for political reasons, for financial gain, and as a diversionary tactic to steal intellectual property. All businesses are potential targets, and the boardroom is beginning to understand not only what but also how much is at stake. Since 2012, IDC has seen a sharp increase in attack frequency, bandwidth volume, application orientation, and duration. Attacks are more sophisticated in nature and in some cases can last for months. These attacks escalated throughout 2014 and attackers continue to find novel vectors and approaches to outwit defenders. Today's attackers are also targeting an ever-widening array of industries and technology implementations.

The increase in complexity and targets drives home the reality that any business can become the target of a DDoS attack and the loss of both revenue and brand equity that can result. In addition, these recent instances highlight a new approach. DDoS can now act as a diversionary tactic, while advanced malware and vulnerability exploitation are simultaneously used to obtain financial information and intellectual property. At the same time, recent seismic shifts in technology — the rise of cloud computing, the Internet of Things, the emergence of software-defined networks — promise to introduce new attack risks and threats.

With the prevalence and duration of attacks on the rise, organizations need to take steps to protect their infrastructure from the advanced methods being employed. IDC believes that volumetric attacks will continue to be common. However, application layer attacks will loom larger in the threat landscape as a result of the relative ease with which they can be launched. Despite the fact that volumetric-based attacks will remain the most common, more advanced hybrid attacks that include application layer and encrypted traffic in addition to volumetric methods will also grow, spurring growth in the use of on-premise equipment.

One promising area of development is the use of hybrid defense. Rather than a "defense in depth" approach where organizations simply have on-premise equipment from one provider and cloud services from another, cobbling together what may resemble to the layperson a complete solution, true hybrid defenses are offered as a single solution leveraging the benefits of both service delivery methods. Hybrid approaches are becoming more widespread as organizations have sought to defend against all vectors of DDoS attacks and as service providers and product vendors have begun to work more closely to deliver synergistic solutions. Better still are hybrid solutions delivered by a single vendor, which have the advantage of robust information sharing between premise-based technology and cloud-based technology that can improve both the speed and the accuracy of mitigation.

DDoS Attack Methods: Recent Trends

DDoS attacks are assaults that flood a network with so many malicious (or illegitimate) requests that regular traffic is either slowed or completely interrupted. These attacks disrupt the availability of network resources and can interrupt network service for extended periods of time.

Typical targets include online businesses with large Web sites, ISP root servers, large enterprises, and service providers. These attacks can cause both direct and indirect damages to the target company. Direct damages include revenue loss and/or increased network costs. Indirect damages are related to intangible factors such as the loss of brand equity, business reputation, and/or customer satisfaction.

In a typical DDoS scenario, hackers use a large number of bot-infected, compromised computers to launch large-scale attacks, often PCs with broadband connections. Once the PCs have been taken over, perpetrators then remotely command them through the use of a botnet command and control channel. The immediate result can be devastating, ranging from service slowdowns to complete shutdowns for hours or even days.

The methods and motivations behind such attacks have evolved noticeably over the course of the past decade. Originally, DDoS attacks centered on brute force tactics, with little focus on stealth or circumventing defenses. An attacker would gain control of a system with an abundance of bandwidth and use it to quickly starve the target of network resources through ping floods, fragmented ICMP packets, or other methods.

As attack exploits evolved and resources became more distributed, motivations changed as well. For example, attacks under the threat of extortion became more prevalent, often surfacing in gaming and gambling venues. Another trend was that "hacktivism" began to play a much more prominent role.

The rise of rentable botnets and easily accessible code such as Low Orbit Ion Cannon (LOIC) exacerbated the problem, making it even easier for a moderately skilled person to launch an attack against any organization the attacker happened to have ideological differences with. The well-publicized attacks against the Church of Scientology and other organizations showcased what a skilled group was capable of and how large the DDoS threat had become.

Today's attacks take on a variety of patterns and sizes. Because of increased botnet accessibility, large attacks are more common, and 20Gbps events have been reported. In addition to an increase in frequency, attacks have also become more sophisticated and stealthy. For example, Layer 7 application attacks are much more targeted and often consist of what appears to be legitimate traffic, making them more difficult to detect. Application layer attacks also require fewer resources to launch.

While they have not begun to outpace network layer events in prevalence, they do represent a significant percentage overall. Many recent attacks feature a combination of methods. For example, a DDoS offensive may begin with a volumetric attack, shift to targeting servers to starve resources, and finally use an HTTP flood. Advanced hybrid and SSL-based encrypted attacks are likely to cause the most disruption.

Another trend is that DDoS attacks are increasingly multivector in nature, meaning they employ a variety of tools and tactics across network DDoS, application DDoS, and Web vulnerability attacks. As an example, Boston Children's Hospital experienced an attack in April 2014 that, although not massive in traffic volume by today's standards, included over 30 vectors, making effective mitigation very complex.

The Benefits of a Hybrid Approach to DDoS Detection and Mitigation

In today's IT environments, there are four mitigation solutions to consider: on-premise, cloud, defense in depth, and hybrid.

On-premise solutions are typically purpose-built, appliance-based products deployed in large enterprise, government, and service provider organizations. Technically, a variety of security products have DDoS prevention capabilities, including routers, switches, firewalls, and intrusion prevention solutions. Unfortunately, these products quickly lose the ability to adequately mitigate DoS attacks of any significant size, especially those directed at the application layer. In fact, these infrastructure components can be directly targeted during DDoS attacks because they quickly become network bottlenecks if dedicated solutions have not been deployed. Dedicated solutions that are deployed in front of other infrastructure devices do not rely on stateful inspection techniques and provide the necessary visibility into the application layer required to adequately defend against on-premise attacks.

The second category is the cloud-based offering. In this case, telcos and cloud providers typically use the same mitigation equipment described previously to build scrubbing centers, where customer traffic can be redirected to filter out attack traffic. These DDoS prevention services are then sold to enterprises and government entities.

While managed solutions are available, customers often become aware of an attack before the service provider and proactively request that their traffic be diverted. This is especially true with "low and slow" attacks where resources may remain technically available but performance is severely impacted. During these attacks, a cloud service may not recognize malicious activity as on-premise IT administrators have better visibility into the situation.

Additionally, when a cloud solution is the only DDoS protection an organization has, an attack of any size requires that traffic be diverted to a scrubbing center. This process is often not seamless, so when an attack continues with little or no interruption for days, or even weeks, traffic has to remain routed to the service provider for that length of time or switch back and forth as the attack ebbs and flows.

The defense in depth scenario is one where an organization extends its on-premise appliances to include cloud signaling to allow for mitigation in cloud-based scrubbing centers. In this scenario, an on-premise appliance provides defense against smaller volumetric attacks and application layer attacks. The level of visibility and quick response offered by being on-premise is arguably much higher, especially in relation to the application layer traffic. That said, large-scale volumetric attacks can quickly overwhelm an enterprise network. If this occurs, the cloud solution is able to divert the traffic into a scrubbing center before rerouting back to the customer network. The on-premise solution provides valuable information about the attack dynamics that the cloud provider can then use to more efficiently clean the traffic.

This solution, however, is often a patchwork by necessity. This can be by choice due to budget constraint. Or it can be due to misunderstanding the technical integration and capabilities of numerous providers. In the end, the buyer is left to believe that it is protected when in actuality it may not be. In addition, the buyer must now manage three or more providers during an attack.

The fourth option is the hybrid solution, which represents a combination of both on-premise and cloud-based approaches used in concert and with seamless integration. This is a newer and more comprehensive approach that a number of organizations are beginning to consider. While true hybrid solutions have not been common in the current market, this is starting to change.

Some DDoS attacks saturate the Internet pipe, while others target applications or even do both. With the hybrid approach, on-premise equipment is able to relay specific information about the attack to the cloud provider to aid in quicker mitigation. The on-premise equipment is also able to better detect application-level targeting and mitigate those aspects of the attack, even if the cloud provider can't address them.

Considering Radware's Hybrid DDoS Solution

Radware's attack mitigation solution is a true hybrid approach that provides both on-premise and cloud protection. At its core is DefensePro, a perimeter attack mitigation device that offers comprehensive and accurate detection and mitigation of threats. Detection of attacks goes beyond typical rate-based measures to include network behavioral analysis and advanced challenge/response techniques. Wide security coverage addresses application-level attacks, network flood attacks, known vulnerabilities, and egress traffic attacks. Application attacks addressed include SSL, HTTP GET/POST, low and slow, and intrusions. Radware's attack mitigation solution also includes a Web Application Firewall, which protects against SQL injections, XSS, and other OWASP Top 10 threats. Radware's solution comes with a centralized management component for consolidating monitoring, forensics, reporting, and attack identification across the portfolio. Finally, Radware's Emergency Response Team (ERT) provides a single point of contact for expert support to mitigate both on-premise and cloud-based attacks.

Mitigation from the full spectrum of attacks is automated and is accomplished by generating real-time signatures and distinguishing between attackers and legitimate users.

When large-scale volumetric attacks threaten to saturate the Internet pipe, Radware's on-premise attack mitigation device alerts the ERT, which works with the customer to divert traffic to the scrubbing center. The solution can also be configured to automate the swing of traffic to scrubbing centers. The on-premise attack mitigation device shares information about the attack (e.g., attack vectors, volume, and attack signature) with the cloud scrubbing devices to more efficiently and quickly scrub the traffic without the delays common with multi-technology hybrid solutions.

The hybrid design leverages Radware's position both at the customer site and in the cloud and enables information sharing between the two locations. Rather than colocating two or more solutions, it integrates detection, response, and mitigation, providing customers a more holistic solution to attack mitigation, especially with the growth of multivector attacks that combine threats to both the network layer and the application layer.

Challenges

Radware is better known as a network equipment vendor that provides application delivery controller (ADC) solutions than as a security technology provider. However, Radware's security portfolio has experienced strong growth and adoption across many core security verticals in the past few years. While this has started to shift perceptions of Radware, work still remains to gain additional mindshare among customers specifically around security.

In addition, DDoS solutions tend to be targeted at very large organizations, so the size of the DDoS prevention market remains relatively small in the overall landscape of security solutions. Competition will be fierce as providers fight for limited purchasing resources. That said, IDC does expect the on-premise market to continue to be robust in both standalone and hybrid scenarios. Radware's hybrid approach should provide a key differentiator versus other equipment providers trying to play catch-up. Additionally, key OEM relationships should help open additional business opportunities and expand the company's product footprint. For example, Radware has had an OEM partnership with Check Point Software Technologies since 2012. Under the agreement, Check Point resells Radware's attack mitigation device as DDoS Protector. Additionally, Radware has integrated its security products into the

Cisco Application Centric Infrastructure (ACI) to enable large enterprises, hosting service providers, and ISPs automated tenant-based application delivery and security services.

Finally, while the market has become much more aware of DDoS threats over the past two years, some still believe the protection features in standard routers, firewalls, and IPS appliances are sufficient. Additionally, portions of the market overlook the importance of holistic protection and focus only on volumetric attack protection. Education will remain an important factor to ensure that the entire addressable market is looking at dedicated solutions to guard against DDoS attacks and understands the benefits that single-vendor hybrid solutions can deliver in defending against today's complex attacks.

Conclusion

Volumetric attacks will continue to be the predominant type of DDoS event because of the relative ease with which botnets can send a bandwidth flood that exceeds what most enterprise infrastructures can handle. Although volumetric-based attacks will remain most popular, more advanced and complex hybrid attacks that include application layer and encrypted traffic in addition to volumetric methods will increase, helping drive growth in the on-premise equipment market.

On-premise equipment married with cloud services in a truly integrated hybrid solution is becoming more prevalent as organizations seek to defend against all vectors of DDoS attacks and as solution providers and product vendors work more closely to deliver joint solutions. Radware's hybrid attack mitigation solution is designed to address the new attack vectors affecting enterprise, government, carrier, and service provider organizations. To the extent that Radware can address the challenges described in this paper, IDC believes the company is well positioned for success in the DDoS prevention market.

ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

For more information on IDC, visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

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