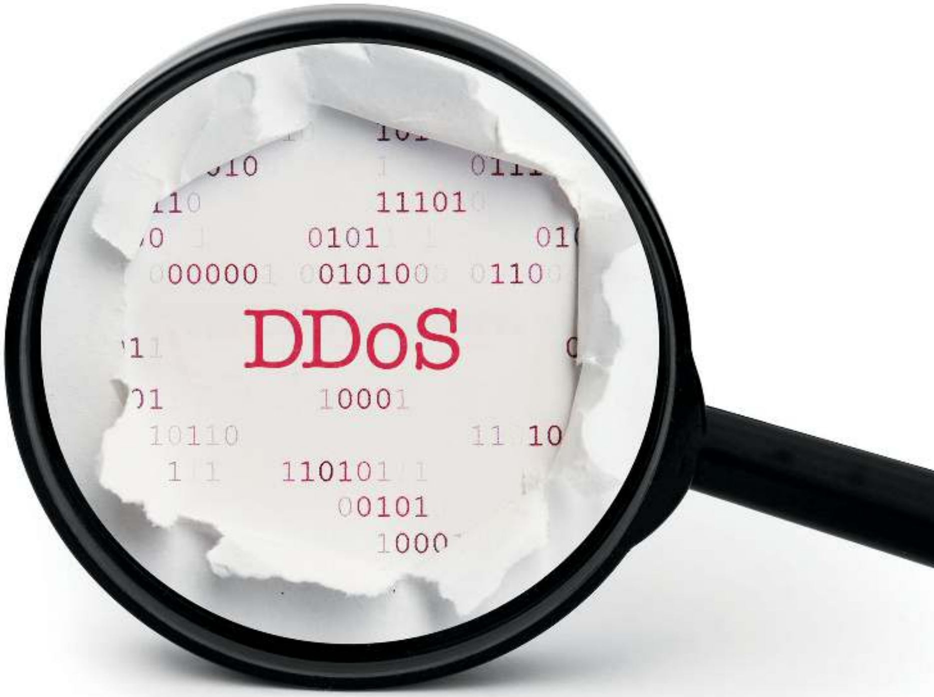
Four Considerations for Addressing the DDoS Risk for Carrier and Cloud Hosting Providers

Whitepaper



SHARE THIS WHITEPAPER

Table of Contents

The Rising Threat of Cyber-Attack Downtime

As distributed denial of service (DDoS) attacks and other cyber-security threats grow exponentially in scale, so must the technologies for defending network and application infrastructure. The size, complexity and frequency of these threats pose a unique challenge and risk to telecommunication carriers, major network operators and large cloud hosting providers. The world's largest and most recognizable enterprises turn to these organizations with the expectation that protection from cyber-security threats is an inherent part of hosting or connectivity services. Unfortunately, making this a reality becomes difficult when the growth of the threats outpace the growth of security products to remedy the risk.

For carriers and hosting providers, 2014 was a watershed year for cyber-security attacks. In addition to dealing with traditional attack vectors, the trend of reflective attacks dramatically increased both the volume of attacks and the number of attacks in the range of 10G to 50G. Such attacks became a common practice as they are easy to generate using the amplification technique. Carriers, who have long dealt with ongoing, low-level attacks targeting customers, were hit particularly hard by this trend. Now, however, the stakes are much higher as targeting the carriers—not customers—prove to be a potentially more effective tactic.

The evolution of attacks is not limited to size; today we see an overwhelming majority of attacks leveraging multiple attack vectors looking for the weakest link within the security environment. In the past, simply providing enough throughput on SYN floods or other common network protocol attack types might have provided sufficient protection. But now attacks are split almost fifty-fifty between network protocols and vectors that leverage layer 7 attack vectors, such as DNS, SMTP or HTTPS.

Recent research from Heavy Reading indicates that 47% of mobile operators in developed markets (North America, Western Europe, Japan, Australia) experience two or more outage or degradation events, lasting an hour or more, caused by malicious attacks. The gold standard that most carriers strive for is 99.999% service availability – this translates to no more than five seconds of downtime a year. Two or more hours of outage or service degradation means they already anticipate falling to 99.97% service availability just based on downtime from malicious attacks.

Four Key Considerations for Addressing Growing Threats

Carrier and hosting providers need to give careful consideration to unique challenges and requirements of DDoS protection in a large carrier or hosting environment. For these organizations, DDoS poses significant risk both to its own infrastructure, and the infrastructure of customers to preserve service level agreements (SLAs) and avoid "collateral damage" scenarios.

Four specific areas that warrant consideration and assessment in determining risk include:

1. Risk of becoming a primary target
2. Risk posed by organizations across the customer base
3. Collateral damage concerns
4. Technology deployment inline across large networks

The Risk of Becoming the Primary Target of an Attack

In its annual Global Application & Network Security Report, Radware looks at emerging threats that pose exponential risk going forward. In the 2014-2015 edition of the report, one such threat is the trend towards attacks against critical infrastructure. In the past, the notion of critical infrastructure has conjured up thoughts of water supply or power generation systems, or networks/systems related to national defense. These systems are increasingly network-reliant and very much a target of cyber-threat. But so are the essential communication networks of any nation, which are almost entirely IP-reliant, a fact not lost on those looking to launch widespread cyber-attack disruption. And as enterprises and public sector organizations move further down the path of cloud deployment for critical production services, this threat rises for the large cloud hosting providers as well.

The Risk Posed by Customers

Threats have expanded to a broader range of industries, organizational sizes and technology deployments. No one is immune. In the past, organizations could make risk-based assessments of individual customers or market segments based on its richness as a target. But as the vertical-focus of cyber-attacks breaks down, so does the notion that as a carrier or hosting provider you are safe if you avoid the "risky industries."

Additionally, there is little distinction between industry and size of attack, based on the availability of inexpensive bots and reflective techniques. According to Radware's 2014-2015 Global Application & Annual Security Report, one in seven attacks was larger than 10G with many exceeding 100Gbps+ in size. Attacks are also evolving to become longer, larger and more sophisticated. Almost 20% of respondents in the Radware report stated they were under ***constant*** attacks in 2014.

Collateral Damage Concerns

Multi-tenancy has introduced a new wave of more efficient network service deployment and delivery. As a result, it has also driven the creation of an entire new industry around cloud-based hosting and computing. But there is a flip-side to these positives. The unfortunate reality of multi-tenancy is that, to a large degree, when one customer becomes the target of an advanced cyber-security threat, many other customers become "collateral damage" risks.

Technology Deployments Across Large Networks

Most technology solutions are built for common enterprise network of data center demands. Therefore, products such as DDoS mitigation equipment tend to scale to support 10 Gbps or maybe 40 Gbps of capacity, as these tend to be the inbound link capacity of high-end enterprise datacenters. But large carriers and cloud hosting providers are operating at a much greater level of scale. They need technology that can better scale without requiring deployment of inordinate amounts of hardware.

Additionally, these organizations face certain restraints around deploying inline appliances at every peering point. As a result, they require solutions architected to accommodate various deployments, from inline data center to geographically distribute Anycast mitigation designs.

Implementing an Attack Mitigation Strategy

Based on the growing threats and impact of attacks, it is clear that carriers and hosting providers need to proactively implement a mitigation strategy. Effective protection from today's DDoS attacks requires a solution that can accurately detect attacks across Layers 3, 4 and 7, quickly initiate mitigation tactics, and address the wide array of attack vectors. For carriers and hosting providers, optimal infrastructure protection will come from a solution that provides real-time and granular mitigation with minimal network changes and no delays due to traffic redirection or flaws in NetFlow detection.

To provide the basis for both own-infrastructure protection and security service delivery, attack mitigation solutions should protect against volumetric, application and encrypted attack vectors. Solutions that provide visibility into application attacks will allow carriers and hosting providers to proactively manage applications before an outage effects a customer.

To support future carrier plans around Software Defined Networks, attack mitigation solutions should support OpenDaylight to allow operators to provision a DoS/DDoS protection service per virtual network segment or per customer.

Finally, an effective solution for attack mitigation needs to integrate easily and seamlessly into existing environments and network/security systems already deployed. Solutions should support integration into provisioning systems and existing customer portals for downstream management for carriers and hosting providers looking to offer services to customers. Organizations should look to vendors with a proven track record of successful technology deployments in Tier 1 carrier and cloud hosting environments.

Implementing an effective strategy for today's volumetric and complex multi-vector attacks can enable a number of valuable use cases for carriers and service providers, including:

- Protection of infrastructure to improve reliability and availability of transit services
- Tenant capabilities that allow for highly customized product sets for different service customers
- Development of new services based on cyber-attack scrubbing capabilities

Radware Introduces the Industry's Most Advanced Attack Mitigation Platform

Radware introduced a new attack mitigation platform that offers carriers and cloud providers the highest attack mitigation performance available on the market. The platform is based on a proven DDoS mitigation engine that delivers unmatched quality of attack detection and mitigation. It provides protection at 230M packets-per-second mitigation capacity with over 300 Gpbs of on-demand throughput scalability. It is the industry's first dedicated attack mitigation platform to support 100Gb interfaces - providing best-in-class attack detection and mitigation with enough capacity for carrier and cloud providers to handle very high volume attacks.

Radware delivers the most complete coverage of all attack types, including common Layer 3, 4 and 7 vectors (SYN, UDP, ICMP, TCP, DNS, SMTP, HTTPS). Many other providers of high capacity mitigation technology focus on one or perhaps a couple of protocols, but this is not comprehensive protection.

The platform is based on proven dedicated hardware that leverages best in a breed real-time behavioral engine to baseline traffic and identify anomalies with minimal false positives. This enables the solution to handle very high volumes of attack traffic without impacting legitimate traffic.

The platform is designed for out-of-the-box, multi-tenant environment support with the ability to support up-to 1,000 active policies, separate processing capabilities and customized management & reporting per tenant.

With its high mitigation capacity, high quality of detection and mitigation, and 100Gb interfaces, Radware's new DefensePro platform is the ultimate choice to fight evolving and growing cyber-attacks at scale for organizations with very large datacenters and inbound link capacity.

For more information about Radware's attack mitigation solutions for carriers and cloud hosting provides, please visit www.radware.com.