Considerations for Choosing a DDoS Mitigation Provider

March 2019

Questions posed by: CenturyLink
Answers by: Martha Gomez Vazquez, Senior Research Analyst, Infrastructure Services

Q Distributed denial-of-service (DDoS) attack sizes are increasing, peaking at 1.3Tbps last year. What should organizations do to ensure their DDoS mitigation providers can handle such attacks?

A The IT environment has become challenging for enterprises as they move through what IDC terms the "3rd Platform" of computing, which integrates cloud, mobile, social, and big data technologies into IT infrastructure applications and business processes. A large DDoS attack can disrupt any of these four critical areas of the 3rd Platform.

Therefore, the IT environment has shifted, becoming more distributed, with applications existing on-premises as well as in private and public clouds. The perimeter has expanded, meaning the attack surface is growing and bringing in more vulnerabilities. As a result of the new IT environment, new types of DDoS attacks can impact a network easily. If organizations don't have enough protection in place, these attacks — application or volumetric — can last hours, days, or even months. In fact, an IDC survey found that 46% of respondents have already experienced an attack. These DDoS attacks run the gamut, including volumetric (56%), TCP state exhaustion (55%), multivector (44%), and application layer (41%).

Organizations should review whether their DDoS mitigation providers can handle these various attacks, specifically in the event of multiple simultaneous assaults on multiple customers. DDoS mitigation providers such as telecommunications providers have a unique position to defend against attacks, especially volumetric attacks, because they can drop the bad traffic entering the network and direct it to scrubbing centers only when needed, thereby reducing latency.
Q What is the advantage of working with a DDoS mitigation provider that has a large global network and a significant peering point footprint?

A The DDoS prevention market includes internet service providers (SPs), telecommunications providers, and content delivery network (CDN) providers or hosts, as well as cloud security service providers and managed security service providers. Organizations choosing a service provider for DDoS protection should consider a provider with a large network that provides the visibility to see attacks occurring in the network from a global perspective. Typically, these providers rely on scrubbing centers to mitigate large volumetric attacks, which can cause latency issues when the traffic is sent to the scrubbing center and then cleaned traffic is returned to the right destination. While scrubbing centers can clean the bad traffic before it reaches an organization’s targeted website, the experienced latency could negatively impact customers.

Utilizing a provider that has a large global network and a significant peering point footprint can deliver a greater benefit because the provider can intercept and mitigate attacks closer to the source than a provider that relies on a smaller footprint. Such service providers have broad network visibility and use the network as a source of attack detection at different peering points for improved performance. Additionally, the same network can be used as the first layer of mitigation for very large attacks with residual attack traffic being handled via scrubbing centers.

Q How important are flexibility and performance in returning clean traffic to customers after filtering out attack traffic?

A DDoS attacks are growing more and more complex. Organizations are looking not only at specific vendors to provide DDoS protection but also at their internet SPs, managed security SPs, and carriers. Managed security SPs, internet SPs, and carriers have a unique ability to see a broad variety of attacks and can stop DDoS threats before they transit the network.

Depending on its requirements, an organization should review how clean traffic is returned and look for providers that can offer more than just GRE tunneling. While returning traffic via GRE tunnels is a good approach, it can have significant limitations such as causing slower performance or latency issues. Service providers that offer more flexible options such as direct and native delivery over existing internet circuits, dedicated transport, or private connectivity can return clean traffic quickly to the customer. These providers have direct access to an internet backbone versus having to deliver clean traffic using over-the-top (OTT) technologies such as GRE that have inherent scalability limitations.
Q: Why should organizations utilize carriers that can take down command and control (C2) infrastructures as one of the approaches for mitigating DDoS attacks?

A: As noted previously, DDoS attacks are becoming more complex, and with the introduction of the Internet of Things (IoT), the attack surface has grown, creating new types of DDoS attacks. With an increasing number of devices connecting to the network, it has become more advantageous for cybercriminals to launch a DDoS attack through a botnet. In the case of the Mirai botnet, for example, the attack was able to hijack IoT devices and cause havoc to other organizations. This style of attack is expected to occur more frequently, so organizations will want their DDoS prevention providers to protect against it. Therefore, it’s important to understand that service providers are differentiated by their ability to see what is occurring on the network. Differentiated service providers that utilize their own threat intelligence to see in advance what is occurring in places such as the dark web have a leg up on the competition. For example, service providers with threat intelligence have the ability to listen to chatter occurring in dark forums. Service providers with such capabilities can take down C2 infrastructure as an additional, highly effective countermeasure to help remove malicious traffic and protect customers.

Q: How should organizations approach protecting big circuits in datacenters that have multiple internet SPs to avoid disrupting normal operations?

A: It is becoming the norm for organizations to utilize multiple telecommunications providers or internet SPs in various regions or geographies based on bandwidth, performance, and availability needs. If a DDoS attack occurs, directing all traffic versus just one carrier’s traffic is operationally less complex and less complicated for the customer. Organizations should look for a telecommunications provider or an internet SP with a holistic approach that is network agnostic, which means that no matter what service provider organizations use, all the traffic can be routed to one provider for scrubbing versus routing each network’s traffic to the respective DDoS mitigation provider. DDoS mitigation providers that are carrier agnostic will also offer multiple return options for affected traffic, which can be scrubbed and then routed back to the customer on any internet connectivity, thereby reducing complexity. Also, DDoS mitigation providers that own the network infrastructure will have greater granularity to filter and scrub the services being attacked rather than redirecting entire blocks of IPs.
MESSAGE FROM THE SPONSOR

As a global communications provider, CenturyLink is in a unique position to defend against DDoS attacks, especially volumetric, as we can drop the bad traffic entering our global network and direct it to scrubbing centers only when needed, reducing latency. Therefore, because of our highly distributed network edge, we can more efficiently shift the first line of defense closer to the threat source.

For example, we can block DDoS attacks upstream at the CenturyLink network edge, nearer to attack traffic origination. We have 43 Tbps of DDoS defense capacity at our network edge and mitigate more than 120 customer DDoS attacks daily.

CenturyLink also has the advanced capability to take down criminal C2 infrastructure that is producing DDoS attacks. Based on our global network visibility combined with advanced threat intelligence produced by our Black Lotus Labs threat research team, we remove ~40 C2s per month to help protect customers and keep the Internet clean.

About the analyst:

Martha Gomez Vazquez, Senior Research Analyst, Infrastructure Services

Martha Gomez Vazquez is a Senior Research Analyst for IDC’s Infrastructure Services research practice focusing on Security Services and Hardware & Software Support and Deployment. In this role, she is responsible for IDC’s worldwide research and analysis on enterprise and service provider security consulting, integration, and managed services as well as hardware and software support and deployment needs.