WHAT IS THE BEST TYPE OF DDoS PROTECTION FOR MY BUSINESS?

If you are asking this question it's likely you already know the frequency of DDoS attacks is on the rise. And just as web-based services have become critical to your business, bad actors have developed more sophisticated attack strategies to threaten their availability.

• • ○

You really have three options: a cloud-based service, on-premise protection, or a layered, hybrid approach combining the two.

ARBOR® NETWORKS
The Security Division of NETSCOUT

CLOUD-BASED MITIGATION SERVICES

CDN vendors who offer DDoS protection do so under the promise of convenience. Use their Always-On service with automated detection and your DDoS problems will be solved. That sounds great until you understand the consequences.

1. Degraded User Experience

In Always-On DDoS mitigation services traffic must be permanently diverted through the cloud mitigation provider's network, whether an attack is present or not. This diversion can degrades the user experience through increased latency.

2. Limited Protocols

Many CDN service providers use reverse proxies to receive suspect traffic; protection is generally limited to HTTP or HTTPS (SSL) protocols. Yet modern DDoS attacks can take many forms, shifting attack vectors to non-HTTP protocols and potentially overwhelming individual proxy nodes leading to partial outages.

3. On-Going Vulnerability

A proxy server must continue to reach the targeted service to retrieve content and supply user data. This means the targeted service is still on the internet and vulnerable to attackers if they discover its true address allowing attackers to completely bypass the cloud mitigation providers network.

4. Premium Cost

Always-On mitigation services must incorporate into the price mitigating every DDoS attack no matter how small. Their service price necessarily presumes each customer will be attacked frequently, leading to high monthly or annual fees and overall, a poor total cost of ownership (TCO) for the customer.

CDN-based DDoS services promise convenience but at what cost?

ON-PREMISE MITIGATION SYSTEMS

Many firewall vendors are now offering DDoS protection. What customers are getting is nothing more than a false sense of security. While firewalls do stop some DDoS attacks — they don't stop them all and they often become the targets of attacks themselves. They are effective tools in addressing network integrity and confidentiality, but with DDoS protection, they provide a false sense of security because they fail to address the fundamental concern regarding DDoS attacks — network availability.

According to *Arbor's 12th Annual Worldwide Infrastructure Security Report*:

- Nearly half of Enterprise, Government and Education (EGE) respondents had firewall or IPS device experience a failure or contribute to an outage during an attack, similar to last year.
- Firewalls, load balancers, and CDNs all tied for last place in effectiveness at mitigating DDoS attacks.
- Sixty percent of EGE organizations estimate that their downtime costs more than $500/minute.

It's clear that relying on firewalls alone can be extremely costly.

DDoS is a complex, dynamic attack type and it requires a purpose-built solution. Intelligent DDoS Mitigation Systems (IDMS) provide greater protection, faster mitigation and more control.

The fact is eighty percent of DDoS attacks are less than 1Gbps, and these can be mitigated faster, many times automatically, via an on-premise IDMS. IDMS can be multi-protocol, meaning they can detect and mitigate whatever attackers throw at the targeted service. Being part of the host network means IDMS can surgically remove attack traffic at the lowest level, before the attack traffic penetrates and impacts any other network component.

Since the majority of attacks can be managed on-premise, the one-time cost of IDMS extends value over many DDoS events, and into the future. Depending upon the degree of intelligence and automation — and the nature of your business — the TCO for IDMS can be less than cloud-based mitigation, certainly less than CDN-based Always-On cloud services.

And keeping traffic out of a third-party network and solely connected to the internet (unlike a CDN) preserves the ideal traffic paths for optimal user experience for all the times a service is not under attack.

SO WHAT DOES A HYBRID APPROACH ADD?

Of course, it is volumetric attacks that have grabbed the headlines, think Mirai. According to respondents of *Arbor's 12th Annual Worldwide Infrastructure Security Report*, the largest attack in 2016 was 800 Gbps. Multi-hundred Gbps attacks have become commonplace. Now that attackers have started exploiting IoT devices in earnest, experts are predicting attacks north of 1Tbps are not far away. Industry analysts are aligned on this point. Industry best practice today requires both on-premise IDMS and cloud-based mitigation. Effective DDoS defense is no longer an either-or question. Leading enterprises' are getting the message; respondents to the 2016 WISR survey indicated a layered, hybrid approach to DDoS mitigation was the fastest growing strategy, increasing 30% over the past year.

Having this multi-layer approach is the right architecture, but tight integration between on-premise solutions with cloud services is the key. When a DDoS attack does saturate the in-bound internet circuit, the on-premise technology should automatically signal the cloud component to temporarily divert traffic to one or more scrubbing facilities. This scrubbing can filter out terabits of attack traffic before securely delivering clean traffic to the target network. This kind integration must be fast, leveraging the cloud for high volume attacks, and removing the ability for attack traffic to overwhelm on-premise defenses.

Understanding that the majority of DDoS attacks can be mitigated by IDMS technology on-premise, a well-integrated cloud component should be considered insurance, not the first line of defense.

• • ○

Learn more read Arbor's DDoS defense overview.

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

AI/PROTECTION/EN/0617-LETTER

Corporate Headquarters
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free USA: +1 866 212 7267
T: +1 781 362 4300

North American Sales
Toll Free: +1 855 773 9200

Europe
T: +44 207 127 8147

Asia Pacific
T: +65 6664 3140

Latin & Central America
T: +52 55 4624 4842