Arbor Edge Defense Complements Any Cloud DDoS Solution for Increased Protection of Critical Services

Cloud DDoS services are great for mitigating large-scale volumetric attacks. But with the breadth and depth of today's DDoS attacks (volumetric, state, and application-layer) happening continuously, one single mitigation solution isn't adequate to protect business-critical services. A multi-layered approach combining on-premise surgical mitigation with intelligent signaling to large-scale cloud mitigation combines the best of both techniques, mitigating attacks of all types and ensuring business continuity.

Challenge

As DDoS attacks continually become larger and more prevalent, cloud-based DDoS mitigation services have become popular choices for customers who need protection that can react quickly and scale effectively. These services commonly come from CDN providers, ISPs or ISP-agnostic DDoS protection services providers. Whether it's always-on or on-demand, cloud-based DDoS scrubbing services are a useful and necessary way of protecting your organization. However, relying solely upon on a cloud-based DDoS protection service is not comprehensive enough to effectively combat all DDoS attacks.

Most DDoS attacks combine volume, application-layer, and state-exhaustion techniques to bring down their targets. Unfortunately, while cloud mitigation solutions are used for stopping high-volume attacks, state-exhaustion or application-layer DDoS attacks can go completely undetected when the volume is low, or the attack patterns are not identified and stopped by the cloud-based mitigation tools responsible for blocking the high-volume attacks. **With cloud DDoS services, users commonly report that some hostile traffic is still seen at the target hosts even when cloud mitigation is active.** Beyond DDoS, any attacks actively targeting services, or malicious traffic from a potentially compromised host or other IoC still not only needs to be detected but stopped. On-premise mitigation is a complimentary and necessary addition to cloud mitigation for protection of business critical services.

Risk

Large volume attacks are easily covered. Unfortunately, dangerous smaller attack traffic is still reaching your business-critical services and networks. That traffic could be state-exhaustion, application-layer attacks, or something even more dangerous such as attempts to compromise hosts or botnet control messaging. Since simple cloud mitigation does very little in stopping state-exhaustion and application-layer attacks and isn't designed to detect or mitigate traffic based on IoCs and threats, your network and services are still vulnerable to both compromise and downtime.

Solution

Arbor Edge Defense (AED) combines threat detection and DDoS mitigation techniques to not only keep you informed of malicious traffic but block it. AED is on-premise, always on, mitigating any attacks which may not be detected by network traffic monitoring tools. With AED there's no delta between the beginning of an attack and the mitigation, whereas pre-provisioned cloud-redirection might take several minutes while BGP route updates occur. If you have to provision or manually redirect your traffic during an attack the window of exposure is much longer. In the event of a large volumetric attack, AED's cloud signaling features can intelligently communicate with a cloud-based mitigation service such as Arbor Cloud or one from your ISP. This feature allows mitigation to rapidly be redirected to the cloud as the volume increases. And everything is easily managed through the same interface.

And while BGP AS-PATH prefixes may direct most of your traffic through the cloud service provider, your ISP may still be sending some traffic straight to you due to BGP pathing preference or local preference configurations. Since AED is always on, and on-prem, it sees all attack traffic; even traffic missed by cloud mitigation. Even your GRE endpoint can be protected by AED – something that cannot be done by any cloud-based DDoS service provider.

Lastly, AED utilizes threat intelligence from the Atlas Intelligence Feed to identify and block IoCs – something cloud mitigation services cannot do, providing the most mitigation and security available both during an attack and even during peacetime.

By combining cloud mitigation such as Arbor Cloud or your ISP with on-premise mitigation with AED, you have the most comprehensive protection available from massive volumetric attacks, subtle state-exhaustion or application-layer DDoS attacks while blocking hostile traffic with IoCs.

"Yes our Provider Cloud Mitigation is always-on, but not always mitigating based on their model. If an attack is detected there is a time delta between the detection and mitigation. From this point of view Netscout has a critical role to always mitigate and protect during the delta."

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECUC_014_EN-2001 09/2020