NETSCOUT®

Arbor Edge Defense is an Essential On-Premise DDoS Solution

Cloud DDoS services are great for mitigating large-scale volumetric attacks. But with the breadth and depth of today's DDoS attacks (volumetric, state-exhaustion, 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.
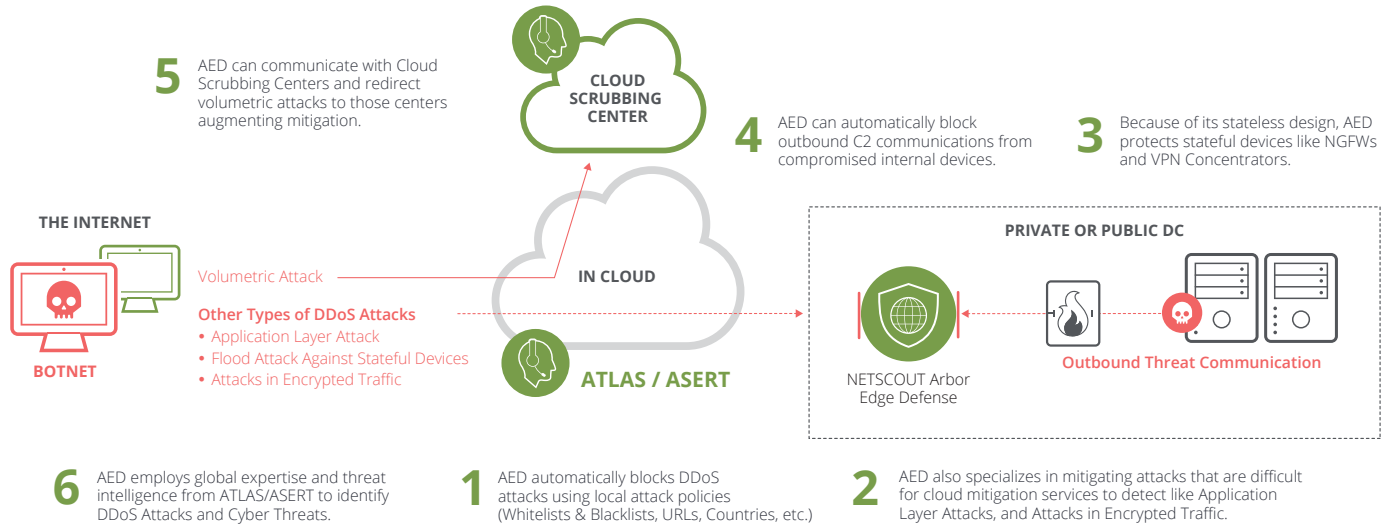
Challenge

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. To augment these cloud solutions, it is essential to add on-premise mitigation capacity to effectively combat all DDoS attacks.

Most DDoS attacks combine volume, application-layer, and state-exhaustion techniques to bring down their targets. Although cloud-mitigation solutions are typically used for stopping high-volume and some state-exhaustion attacks, some state-exhaustion and most 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. 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 necessary addition to cloud mitigation for protection of business-critical services.

Risk

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 cloud mitigation does little in stopping lower-volume 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.

5 AED can communicate with Cloud Scrubbing Centers and redirect volumetric attacks to those centers augmenting mitigation.

CLOUD SCRUBBING CENTER

4 AED can automatically block outbound C2 communications from compromised internal devices.

3 Because of its stateless design, AED protects stateful devices like NGFWs and VPN Concentrators.

THE INTERNET

Volumetric Attack

IN CLOUD

PRIVATE OR PUBLIC DC

Other Types of DDoS Attacks
• Application Layer Attack
• Flood Attack Against Stateful Devices
• Attacks in Encrypted Traffic

ATLAS / ASERT

NETSCOUT Arbor Edge Defense

Outbound Threat Communication

BOTNET

6 AED employs global expertise and threat intelligence from ATLAS/ASERT to identify DDoS Attacks and Cyber Threats.

1 AED automatically blocks DDoS attacks using local attack policies (Whitelists & Blacklists, URLs, Countries, etc.)

2 AED also specializes in mitigating attacks that are difficult for cloud mitigation services to detect like Application Layer Attacks, and Attacks in Encrypted Traffic.

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. Since cloud-mitigation solutions are designed for high-volume attacks, pre-provisioned 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. Having an on-premise mitigation solution like AED can assist in the mitigation of attack traffic getting through while redirection is taking place. In the event of a large volumetric attack detected at the network edge, 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-premise, it sees all attack traffic — even traffic missed by cloud mitigation. Even your GRE endpoint can be protected by AED.

Lastly, AED utilizes threat intelligence from the Atlas Intelligence Feed (AIF) to identify and block IoCs, 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®