Stopping Application-Layer DDoS Attacks

An application-layer DDoS attack is a form of DDoS attack where attackers target application-layer processes. The attack over-exercises specific functions or features of an application or website with the intention to disable those functions or features – resulting in the application not being able to deliver content to the user. These attacks are particularly insidious because they can be very effective with as few as one attacking machine generating a low traffic rate, which appears legitimate and makes them very difficult to detect and mitigate.

Threat

The legitimately disguised traffic employed by application layer DDoS attacks is designed to slow application servers and tie up server resources while also evading detection and mitigation. To accomplish this, these attacks typically conform to the protocols the applications are using, which often involves protocol handshakes and protocol/application compliance. An example of this type of attack would be a SLOW POST attack where the attacker sends legitimate HTTP POST commands from a multitude of compromised machines that are compliant but the message body is sent at a painfully low speed meaning the server will subsequently slow to a crawl due to the overload or exhaustion of the servers connection state table. Because the traffic within the attack appears to be legitimate, operators may not be looking for them or may not be prepared to use their mitigation solution to block them. In fact, some approaches to DDoS mitigation, such as cloud-based solutions, will not detect such activity or can create a a false positive problem – blocking legitimate users while trying to block attacks adding to the confusion of the attack itself.

These attacks will primarily be launched using botnets especially Internet of Things (IoT) devices.

Risk

Not only have attackers added complexity with increased size and scope of botnet armies, complexity within each attack has also increased by combining various attack vectors in a single campaign. Application-layer attacks are employed in these campaigns in a variety of ways. Sometimes they are used to distract IT and security personnel from other security breaches taking place at the same time, such as malware intrusion. And sometimes the volumetric attacks are the distraction to hide the more focused application-level attacks, which do the real damage.

Investigation

A strong defense posture calls for protection against all types of threats without setting a priority on any one type of attack since they all can do damage to your critical business processes. Ignoring any one of them leaves you exposed at some point along the risk continuum. The most common form of DDoS attack protection today is a cloud-based mitigation service, often from ISPs or independent providers. And while such services are indeed vital to stop large, volumetric DDoS attacks that outstrip the volume of internet circuits, that is only one part of a comprehensive protection strategy.

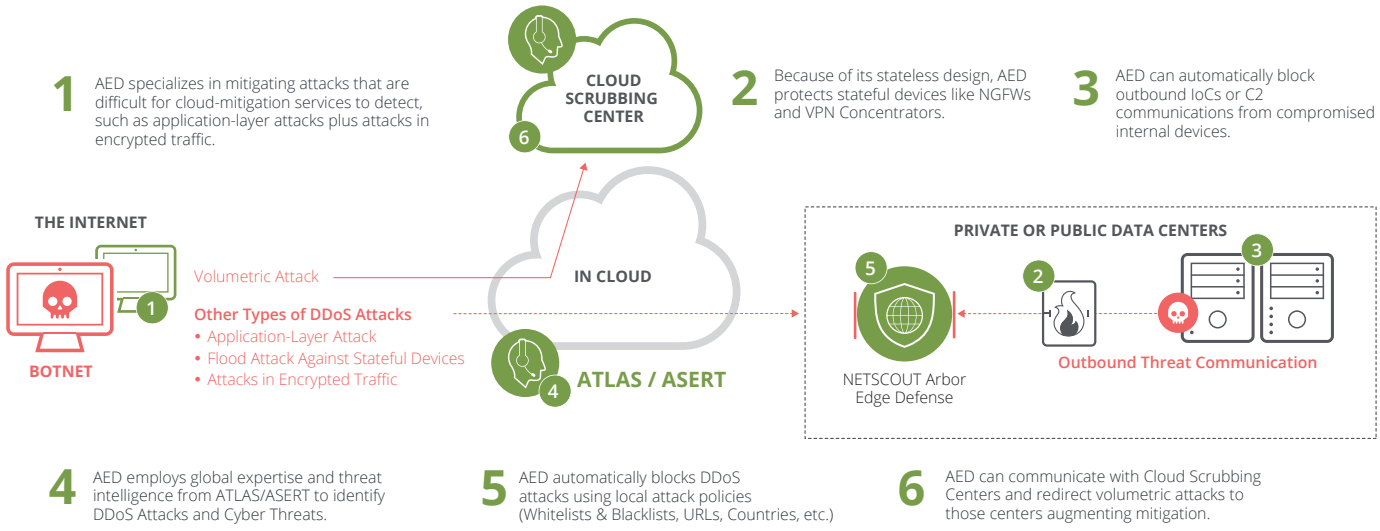

Figure 1: NETSCOUT AED provides a first and last line of network edge and application layer defense.

Mitigation

The other part of a comprehensive DDoS protection strategy must focus on attacks that cloud solutions are not equipped to detect in a timely manner. Due to the impression of legitimate traffic employed by application-layer attacks, they will not automatically trigger attack traffic rerouting employed by cloud-scrubbing solutions. Additionally, cloud solutions are not typically equipped to monitor the encrypted HTTP traffic that makes up most of the application-layer traffic mainly because most networks do not want their authorized certificates residing in the cloud, nor do cloud vendors want the responsibility of managing their customers certificates.

Defending against both these situations requires a device that can distinguish between legitimate traffic coming into a network and cleverly disguised threats while also having the ability to decrypt, scan and re-encrypt all traffic as it comes through the edge of the network. Arbor Edge Defense® (AED) accomplishes both of these objectives. To test traffic for legitimacy, AED employs a combination of traffic profiling techniques so it can track and block abnormal activity, while also deploying progressive security challenges. By issuing a requirement such as a JavaScript computational challenge to the requesting machine, it is possible to test if a bot is involved in an application-layer attack, and thus mitigate that attack if it is. Because AED is in an always-on posture, it can decrypt all encrypted traffic for the purpose of monitoring for attacks and then re-encrypt as it moves the clean traffic along. Additionally, a dedicated, edge-based DDoS protection solution like AED allows you to fine tune the protections so that they won't block legitimate application traffic or have an impact on normal users, even during an attack.

Finally, because of AED's access to NETSCOUT's unique DDoS threat intelligence, it can effectively and automatically block application-layer attacks by identifying known botnet hosts and blocking known sources of DDoS attack traffic, including application-layer attacks. This provides a unique and effective way to help stop application-layer attacks that might trick conventional DDoS protection solutions. Only NETSCOUT has the global DDoS attack intelligence that enables this kind of intelligent, automated blocking. AED is widely considered to be the best-of-breed, on-premises, stateless solution for DDoS attack identification and mitigation.

Summary

A hybrid or layered defense combining on-premises and cloud-based detection and mitigation, informed by global threat intelligence alerts and powered by automation, is widely considered best practice for detection and mitigation of all DDoS attacks, including application-layer attacks

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_018_EN-2101 12/2021