Stopping Attacks in Encrypted Traffic

Encryption is one of the most basic necessities in the security arsenal. It's what makes it possible for banks to offer online banking and funds transfers, or for consumers to make purchases online using their credit or debit cards. It's what protects the public's online interaction with government agencies or health care providers. Such services enable access to a wealth of personal, confidential, and financial data. So it should surprise no one that encrypted services are prime targets of DDoS attacks. Identity thieves and cyber criminals can have a field day if they succeed in breaking web service encryption.

Threat

According to NETSCOUT® Arbor's 13th Annual Worldwide Infrastructure Security Report (WISR), attacks targeting encrypted web services have become increasingly common in recent years. Among enterprise, government, and education (EGE) respondents, 53% of detected attacks targeted encrypted services at the application layer. And 42% of respondents experienced attacks targeting the TLS/SSL (Transport Layer Security/Secure Socket Layer) protocol governing client-server authentication and secure communications.

One helpful statistic coming out of the 13th WISR though, is that enterprises are recognizing that traditional firewalls and intrusion prevention systems are insufficient in confronting sophisticated DDoS attacks – particularly encrypted attacks targeting encrypted services. Encryption is essential but cannot be relied upon on its own to thwart determined and sophisticated attackers. Given the critical nature of most encrypted applications and services, a single successful attack can have devastating consequences.

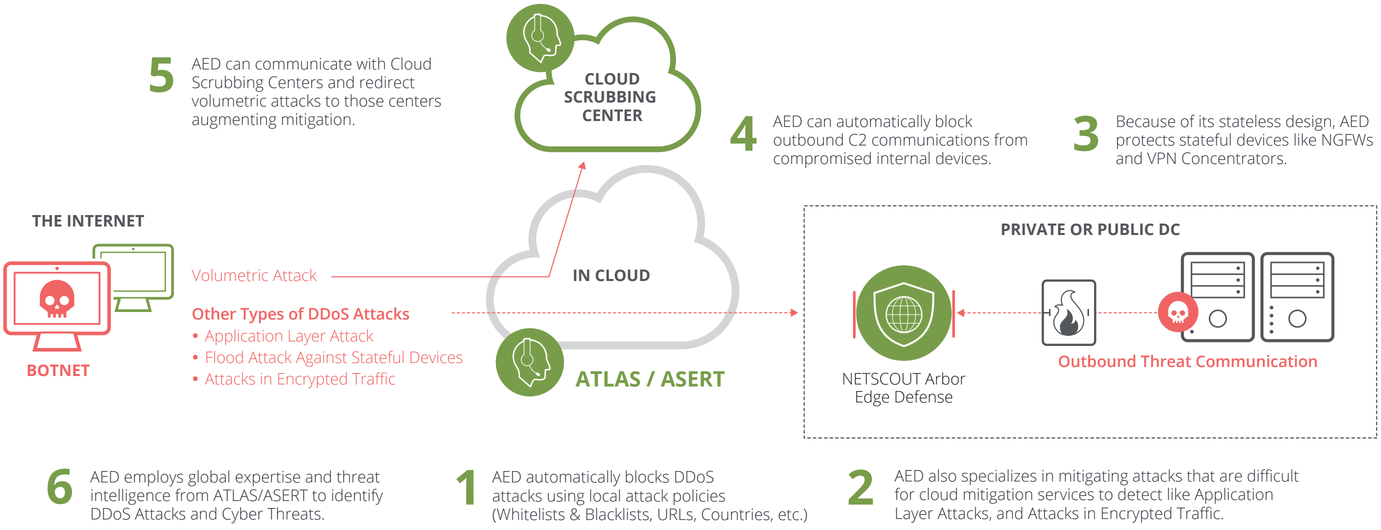
Risk

Reputational and brand damage are frequently cited as the worst consequences of a DDoS attack. Additionally, nothing could be more damaging to an organization's reputation than to compromise the secure services like banking or online purchases that consumers have come to trust and rely upon every day with hardly a second thought. Institutions need to take measures that go beyond encryption to ensure the integrity and availability of their most critical services and continued creditability of their reputation and brand.

Investigation

DDoS attacks targeting encrypted services tend to fall into four categories:

- Attacks that target the SSL/TLS negotiation, commonly known as the "handshake," which determines how two parties to an internet connection will encrypt their communications.
- Protocol or connection attacks against SSL service ports, which seek to exploit SSL vulnerabilities.
- Volumetric attacks targeting SSL/TLS service ports, which overwhelm port capacity with high-volume traffic floods.
- Application-layer attacks against underlying service running over SSL/TLS.


CLOUD SCRUBBING CENTER
THE INTERNET
BOTNET
Volumetric Attack
Other Types of DDoS Attacks
• Application Layer Attack
• Flood Attack Against Stateful Devices
• Attacks in Encrypted Traffic
IN CLOUD
ATLAS / ASERT
PRIVATE OR PUBLIC DC
NETSCOUT Arbor Edge Defense
Outbound Threat Communication

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

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.

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.

Attackers are unrelenting in their assaults on high-value encrypted targets. To make matters worse, attackers often use SSL/TLS encryption themselves to hide nefarious activity. The high volumes of encrypted internet traffic that traverse networks without being inspected, make it easy for malicious actors to hide among legitimate traffic, all while preparing to unleash attacks on secure HTTPS services. A key component of a security arsenal, therefore, is the ability to decrypt and inspect encrypted traffic securely and attest to its authenticity without slowing, disrupting or compromising legitimate traffic.

Another area of concern regarding decrypting and scanning packets is where their decryption is executed. Many organizations do not want their traffic being decrypted off site or by a cloud service because it may require sharing private certificates with the cloud provider, which is a security risk that many Enterprises aren't willing to take. In some situations, cloud providers themselves don't want to have to be responsible for managing private keys and the associated liability risks if the keys are leaked or exposed from their systems.

While decryption is not always necessary for successful mitigation, there is clearly a growing need for scalable solutions for decrypting packets that will expose malicious traffic.

Mitigation

Operators and hosts of secure web services increasingly recognize the need for purpose-built on-premise DDoS Mitigation Systems as the only effective option for mitigating DDoS attacks on encrypted traffic. NETSCOUT Arbor Edge Defense® (AED) allows the Enterprise to segment the decryption and application-layer mitigation (which often is done at lower volume) from the cloud while still having the cloud service for coverage against volumetric attacks. AED's decryption capabilities, include support for Perfect Forward Secrecy (PFS) through an active TLS Proxy, dedicated hardware-based decryption, and support for many different cipher suites.

Summary

Understanding the impact a DDoS attack against secure encrypted services could have on your organization's reputation and brand should be enough to drive an initiative to find a solution. Having the knowledge that decrypting traffic for inspection in the cloud could lead to potential degradation of the security of the organization's private keys should bolster the need to execute decryption, inspection, and re-encryption with an on-premise, purpose-built DDoS-mitigation solution like AED.

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