S.x DOS and DDOS Mitigation

Overview

Research into scenario of low traffic application unintentional DOS and mitigation services.

Types of Attacks

http://www.cyberdefensemagazine.com/choosing-a-ddos-mitigation-solution-the-cloud-based-approach/#sthash.XIwsFI8a.dpbs

Volume Based Attacks –The attacker's try to saturate the bandwidth of the targets flooding it with a huge quantity of data, the category includes ICMP floods, UDP floods and other spoofed-packet floods. This type of attack is very common and very simple to realize thanks to the huge quantity of tools available for free on the Internet, the technique is very popular in the hacktivist underground. Volume Based Attacks magnitude is measured in bits per second (Bps)

Protocol Attacks –The attacker's goal is to saturate server resources of the targets or those of intermediate communication equipment (e.g. Load balancers) exploiting network protocol flaw. The category includes SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS and more. The Protocol Attacks magnitude is measured in Packets per second.

Application Layer Attacks – The attackers target HTTP trying to exhaust the resource limits of Web services. Application Layer Attacks target specific Web applications flooding them with a huge quantity of requests that saturate target's resources. Application Layer attacks are **hard to detect** because they **don't necessarily involve large volumes** of traffic and require fewer network connections with respect to other types of DDoS techniques. Some example of Application Layer DDoS attacks is Slowloris, and DDoS attacks that target Apache, Windows, or OpenBSD vulnerabilities. Application Layer Attacks magnitude is measured in Requests per second.

Layer 7

http://ddosattackprotection.org/blog/layer-7-ddos-attack/

A Layer 7 DDoS attack uses the seventh protocol of the OSI Model to **target the application interface**, in the process **mimicking real, human behavior that is harder to detect and mitigate**.

https://blog.sucuri.net/2014/02/layer-7-ddos-blocking-http-flood-attacks.html

Attack sample protected using WAF

Akamai

Kona Site Defender: Kona Site Defender is designed to improve the security posture of the Customer's Sites and Applications, and reduce the likelihood and impact of security events by mitigating attacks in the Akamai network prior to reaching the Customer's origin infrastructure. Kona Site Defender includes configurable functionality designed to help protect Customer Sites by reducing the risk and impact of attacks at the network and application layers. Kona Site Defender provides r**ate control protections** to mitigate the risk of Denial of Service and Distributed Denial of Service attacks as well as **common attack methodologies** such as SQL Injection, Cross-Site Scripting, Trojan backdoors, and **malicio us bots**. Kona Site Defender provides tools that enable the **definition and enforcement of security policies specific to client IP**, HTTP method and other **request parameters**. Kona Site Defender is also designed to provide protection from burst charges associated with unexpected or malicious traffic spikes. Kona Site Defender includes Kona Web Application Firewall, Site Shield, Site Failover, Access Control, Security Monitor, Compliance Management and DDoS Fee Protection

Konda Product Description

p5 Enables **inspection** of HTTP Request/Response Headers and **HTTP POST Request/Response Bodies** through a series of **cascading REGEX rules in order to protect against attacks** such as SQL Injections and Cross-Site Scripting.

Bad Robots - **Detects requests by malicious automated programs such as robots**, crawlers, and security scanners. Malicious automated programs collect information from a web site, consume bandwidth, and might also search for vulnerabilities on the web site. Detecting malicious crawlers is especially useful against comment spam.

p6 Rate Controls - Kona Site Defender enables a customer to protect both their websites and applications against DDoS attacks by monitoring and c**ontrolling the rate of requests against the Akamai Intelligent Platform™** and customer Origin. **Rate Categories can be incorporated as WAF rules** thus enabling the customer to dynamically alert and/or block clients exhibiting excessive request rate behaviors. **Requests are controlled based on behavior pattern** – not request structure. Customers can avoid false positives by viewing user agent, cookies, and **session ID within the rate control**. The Rate Control feature allows the Akamai edge server to **differentiate between bots and proxies and identify attacker hiding behind proxies**. Kona Site Defender can respond to bursts of requests within seconds. Rate Controls further protect customers by mitigating Slow POST DDoS attacks. POST requests are not sent to the origin until the POST body completes at the edge. POST bodies that take too long to complete are terminated.

Evolving Threats Whitepaper

Application Layer Controls - Application Layer Controls include a collection of **pre-defined yet configurable web application firewall rules** for different types of attack categories. These rules also **enable deep packet inspection of an HTTP/S Request/Response** and its **payload** in order to identify and protect against attacks such as SQL Injections, Cross-Site Scripting, etc.

Rate Controls provides protection against application layer DDoS attacks by monitoring and **controlling the rate of requests** against the Akamai Edge servers and the customer origin. Rate categories can be **incorporated as WAF rules** enabling the customer to **dynamically alert and/or block clients** exhibiting excessive request rate behaviors. Statistics are collected for 3 request phases: **client request**; forward request; and forward response.

References

Amazon White Paper- https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf