Common Attack Methods

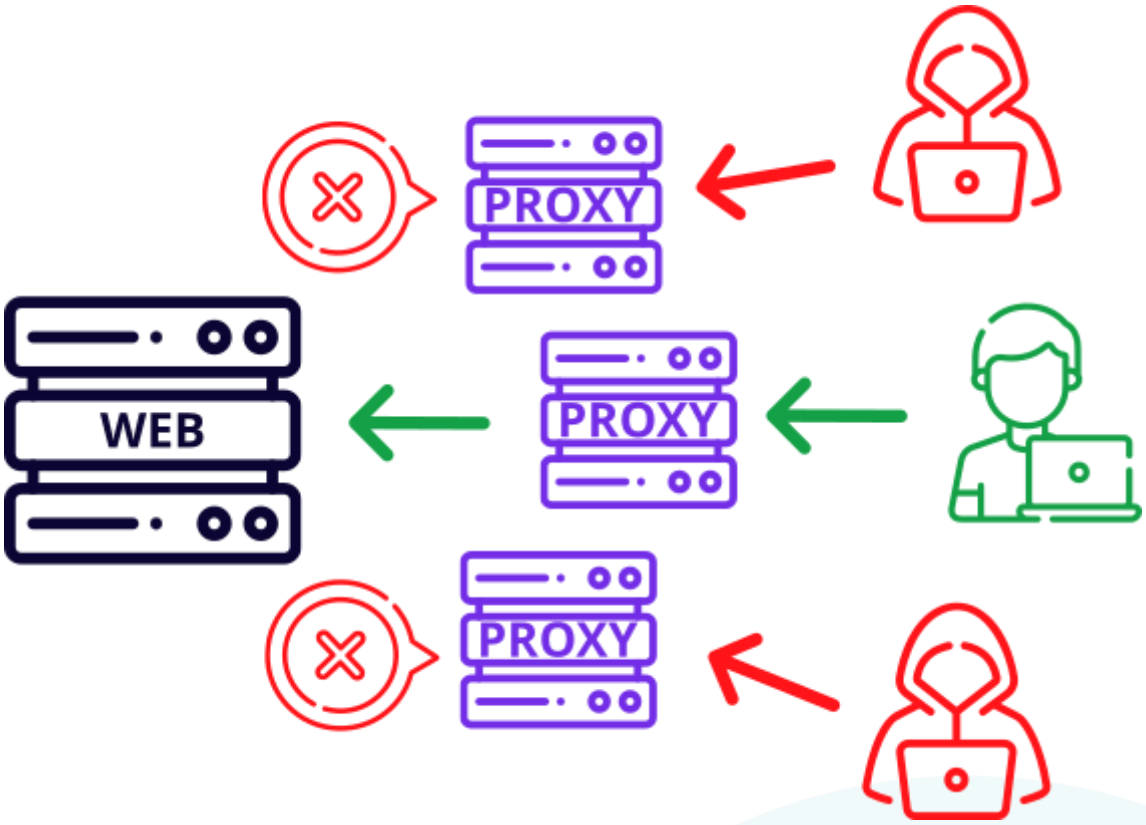
Anycast proxies alone are not a complete security solution, but they form a strong first line of defense. Their primary strength lies in traffic distribution, early termination, and filtering. When combined with additional controls such as Web Application Firewalls (WAFs), rate limiting, and bot management—all of which are provided by WEDOS.protection—Anycast proxies become part of a comprehensive security strategy.

Distributed Denial of Service (DDoS) and Botnet Attacks

DDoS attacks are among the most common types of cyberattacks. Attackers aim to overwhelm a single endpoint, such as a web server, by flooding it with large volumes of malicious requests, preventing legitimate users from accessing the service.

DDoS attacks include volumetric attacks, such as UDP floods, SYN floods, or amplification attacks, which typically originate in different locations, but converge on the single endpoint. Anycast routing distributes incoming traffic across many geographically dispersed edge nodes. Each node absorbs a portion of the attack, significantly reducing the risk of service disruption. Proxy servers at the edge apply rate limiting and traffic filtering to further mitigate the attack.

b2b@wedos.com
WEDOS.com
WEDOS Group SA
7 Rue Robert Stümper
L - 2557 Luxembourg
Luxembourg
EU

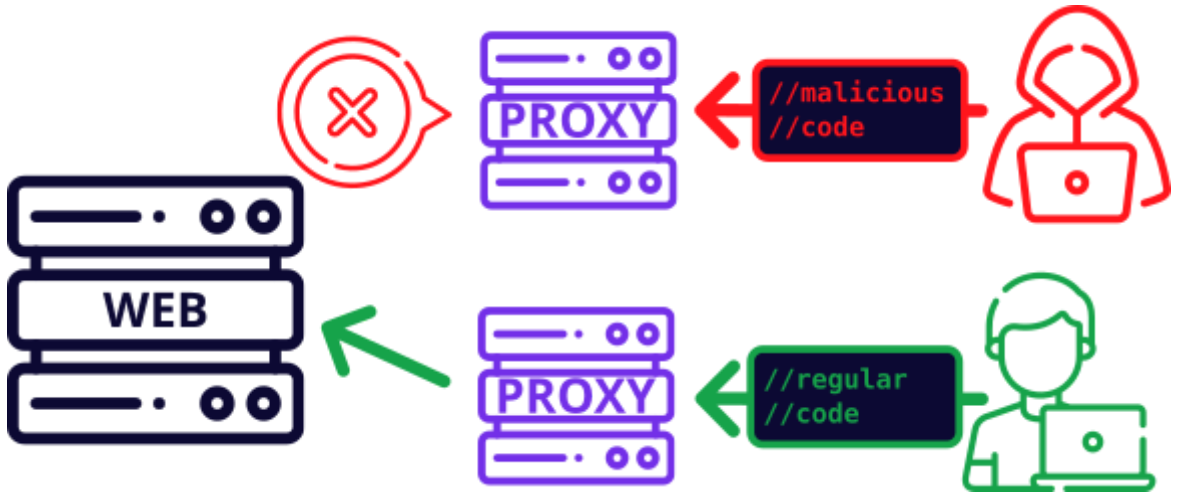


Large botnets generate attack traffic from many regions simultaneously. Anycast routing naturally directs this traffic to the nearest edge node. The nodes cooperate to identify abnormal traffic patterns and bot signatures across the Anycast network.

Application-Layer (Layer 7) Attacks

Application-layer attacks are more targeted and sophisticated than other DDoS attacks. Techniques such as HTTP floods and API abuse attempt to mimic legitimate user behavior in order to bypass basic filtering. Anycast proxies terminate connections at the edge based on WAF (Web Application Firewall) rules, validation and behavioral analysis, filtering requests before they reach the target server.

b2b@wedos.com
WEDOS.com
WEDOS Group SA
7 Rue Robert Stümper
L - 2557 Luxembourg
Luxembourg
EU



Brute-Force and Credential-Stuffing Attacks

Brute-force and credential-stuffing attacks involve high-volume authentication attempts against login endpoints, such as wp-admin or API authentication paths. Anycast allows per-region or per-node rate limiting and anomaly detection, throttling or blocking attackers locally without affecting global users.

Reconnaissance and Scanning Activity

Anycast proxy servers also help mitigate reconnaissance activities such as port scanning, protocol probing, and service fingerprinting. By hiding the origin server's IP address, the proxies reduce the exposed attack surface. Edge nodes detect and drop scanning behavior early, preventing these requests from reaching core infrastructure and limiting attackers' ability to gather useful information.

b2b@wedos.com
WEDOS.com
WEDOS Group SA
7 Rue Robert Stümper
L - 2557 Luxembourg
Luxembourg
EU