Application DDoS

https://campus.barracuda.com/doc/86543210/

A Denial of Service (DoS) attack is a cyberattack in which an attacker makes a web application unavailable to its intended users – effectively denying service to them. These attacks are typically accomplished by flooding the target application with fake traffic or requests from many sources, in an attempt to overload systems and prevent legitimate traffic from reaching the application server.

In a *Distributed* Denial of Service (DDoS) attack, the attacker uses many different sources for the fake traffic – typically tens or hundreds of thousands. This makes it difficult to stop the attack by identifying and blocking a list of sources. A DDoS attack can be likened to sending a crowd of people to a retail store, who stand and block the entryway, preventing legitimate customers from entering.

There are two different types of DDoS attacks:

- Application attacks, which target your application server
- Volumetric attacks, which, along with your application server, target your network infrastructure, including routers, firewalls, switches, and internet links

The Barracuda Web Application Firewall provides comprehensive protection against Application DDoS attacks. To protect your web application from Application DDoS attacks, configure the features described in this section of the Barracuda Web Application Firewall documentation.

For Volumetric DDoS attacks, that attack more than just your application server, the Barracuda Web Application Firewall works with Barracuda Active DDoS Prevention for more complete protection.

Refer to the following sections of the Barracuda Active DDoS Prevention documentation for more information:

- Overview
- What is Active DDoS Prevention?

For more technical information on DDoS attacks, see Distributed Denial-of-Service (DDoS) Attack - Technical Description.