Overview

https://campus.barracuda.com/doc/73700668/

Barracuda Active DDoS Prevention is a service that protects you against volumetric DDoS attacks. Combined with the Application DDoS protection features of the Barracuda Web Application Firewall, Barracuda Active DDoS Protection gives you comprehensive protection from all types of DDoS attacks.

What is Distributed Denial of Service (DDoS)?

Distributed Denial of Service (DDoS) attacks have become a tool of choice for malicious organizations worldwide. Distributed Denial of Service attacks are different from Denial of Service attacks.

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. Denial of Service attacks are typically accomplished by flooding the target application with fake traffic or requests, 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.

Application vs. Volumetric DDoS Attacks

An ***Application* DDoS attack** is a sophisticated strike in which an attacker takes advantage of a known performance problem in your application to overload it. For example, an attacker might find a function of the application that performs a performance-heavy query (like a full text search), and repeatedly trigger that function, thereby overloading the database.

Application DDoS attacks target your application server.

A ***Volumetric* DDoS attack** is a less sophisticated attack, in which an attacker floods your application server with a large amount of fake traffic. The server immediately rejects the traffic; but with a sufficiently large amount of traffic, the time it takes to merely inspect and reject the traffic is enough to overload the application server, making it unable to serve legitimate requests.

Volumetric DDoS attacks target not only your application server, but also your network infrastructure,

including routers, firewalls, switches, and internet links.

Volumetric DDoS Attacks and Microsoft Azure

Barracuda WAF-as-a-Service is deployed in Microsoft Azure, with all of its traffic routing through Azure regions. This routing protects your organization by harnessing the full power of Azure's volumetric DDoS capacity – currently tens of Terabits – orders of magnitude higher than any of the known largest DDOS attacks. Barracuda WAF-as-a-Service integrates with Azure's volumetric DDoS capabilities and adds application-layer DDoS capabilities, to provide full-spectrum protection. Barracuda Networks' application-layer protection feeds data back to Azure's volumetric protection, ensuring that even large application-layer attacks are handled without overwhelming your system.

Volumetric DDoS and the Barracuda Web Application Firewall

The Barracuda Web Application Firewall includes comprehensive protection against Application DDoS attacks. Refer to Application DDoS in the Barracuda Web Application Firewall documentation for details.

Volumetric DDoS attacks impact your network infrastructure, right at your Internet edge, before reaching your Barracuda Web Application Firewall. It is essential to have a dedicated infrastructure to receive and filter huge amounts of traffic to mitigate large volumetric DDoS attacks before they ever reach your infrastructure.

For more information on how Active DDoS Prevention protects your system, refer to What is Active DDoS Prevention?