

Distributed Denial of Service (DDoS)

<https://campus.barracuda.com/doc/76284956/>

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.

The DDoS component includes the following sections:

- [Basic](#)
- [Allow List](#)
- [Block List](#)
- [Web Scraping](#)
- [Slow Client](#)
- [Client Evaluation](#)

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.