DDOS

Common questions about DDoS (Distributed Denial of Service)

What is DDoS?

DDoS is a type of DoS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.

There are two most popular methods to attack a server: SYN flood and Amplified.

SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

DNS amplification is a Distributed Denial of Service attack in which the attacker exploits vulnerabilities in domain name system servers to turn initially small queries into much larger payloads, which are used to bring down the victim’s servers.

SYN flood attacks are practically impossible to pin-point due to the fact that it's very difficult to determine which IP address is a unique website visitor, and which is simply part of the attack.

Amplified attacks are stopped by nullrouting the IP address being attack and keeping it in the blackhole until the attack stops.

Do you provide protection from DDoS?

Every dedicated server from CherryServers gets generic Amplified DDoS (aka Reflection DDoS) protection at no charge. Traffic towards your server is scrubbed from NTP, SSDP, CharGen, DNS and several others well-known reflection attacks.

Do you monitor network activity?

Network activity is monitored 24/7 by network and support teams both. We have numerous tools implemented to assist in detecting and resolving any network shortages that may happen.

How can client add additional DDoS protection layers?

There is a possibility to order a cost-effective CloudFlare service (https://www.cloudflare.com/) for your web site screening. For additional charge we can block all traffic towards your server except known-legal CloudFlare traffic. Also,

we recommend to get additional IP's or a cheapest Smart server for production server management communication.

Another possibility is to set-up a high level of protection and pass all traffic through a traffic cleaning center based on Arbor (High-end security appliance) for an additional price. This is the best choice if your project receives high amount of DDoS attacks, as it will give you absolute protection.

For further information please contact your personal account manager.

How do we protect the world from DDoS attacks?

Requests from IP addresses residing in Spamhaus BCL or EDROP lists are dropped automatically;
High level of outgoing packets per second invokes a temporary disconnection of server‘s traffic;
Requests from Spoofed source IPs are dropped.

Unique solution ID: #1138
Author: Lukas Kalvėnas
Last update: 2017-03-20 14:36