May 8, 2020

DDos Mitigation using Nginx

# What is DDos Attack?

Attempt to make a service unavailable or spike up cost of server resources

## Characteristics

### Bombarding traffic to server using multiple machine typically using bots

### Opening concurrent small connections with server on large scale

### Sending multiple request with large payloads

# nginx configurations to avoid ddos

### **Limiting the Rate of Requests**

Add in nginx.conf

*limit\_req\_zone $binary\_remote\_addr zone=engine:10m rate=2r/s;*

### *limit\_req\_zone $binary\_remote\_addr zone=static:10m rate=100r/s;*

### **Limiting the Number of Connections**

You can limit the number of connections that can be opened by a single client IP address,

Here we tweak the ***limit\_conn\_zone*** and***limit\_conn*** directives to limit the number of connections per IP address.

Add in nginx.conf

*limit\_conn\_zone $binary\_remote\_addr zone=perip:10m;*

*limit\_conn perip 100;*

### **Closing Slow Connections**

## # maximum time between packets the client can pause when sending nginx any data

## client\_body\_timeout 10s;

## # maximum time the client has to send the entire header to nginx

## client\_header\_timeout 10s;