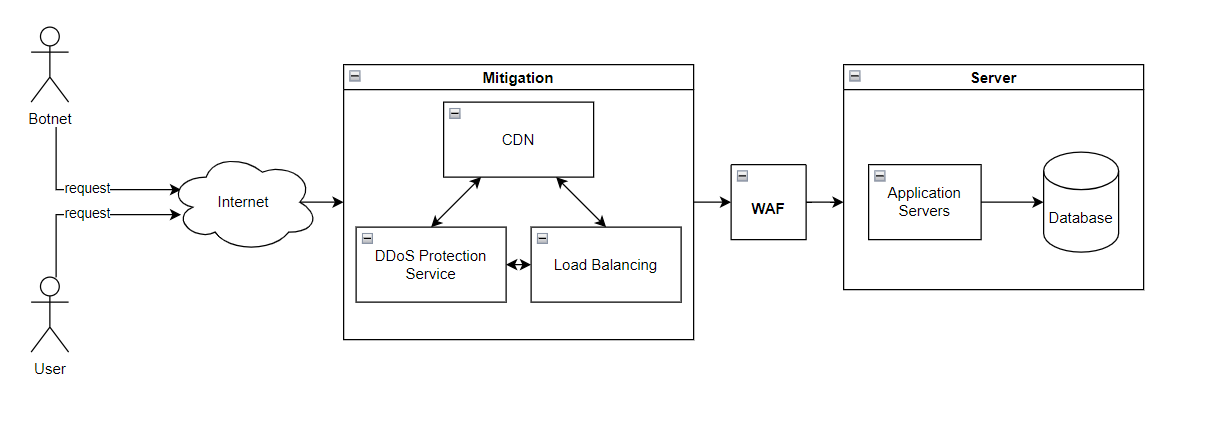
22520136 – Nguyễn Thanh Bình



Để bảo vệ hệ thống Ecommerce của công ty bạn khỏi các cuộc tấn công DDoS, có thể sử dụng mô hình tổng quan sau:

Mô hình tổng quan gồm các thành phần

1. Client: Người dùng truy cập vào hệ thống.

2. CDN (Content Delivery Network): Phân phối nội dung và giảm tải cho máy chủ chính.

3. WAF (Web Application Firewall): Bảo vệ ứng dụng web khỏi các cuộc tấn công.

4. Load Balancer: Phân phối lưu lượng truy cập giữa các máy chủ.

5. DDoS Protection Servic: Dịch vụ bảo vệ chống DDoS chuyên dụng.

6. Application Servers: Máy chủ ứng dụng xử lý yêu cầu từ người dùng.

7. Database Servers: Máy chủ cơ sở dữ liệu lưu trữ thông tin.

Giải pháp chống DDoS

1. CDN (Content Delivery Network): Các dịch vụ CDN có thể kể như Cloudflare, Akamai hay Fastly giúp giảm tải ddos bằng cách chia các gói request qua nhiều máy chủ trên thế giới, giúp giảm tải băng thông và tăng cường bảo vệ bởi DDoS bằng cách phân tán lưu lượng truy cập..

2. WAF (Web Application Firewall): Bảo vệ ứng dụng web khỏi các cuộc tấn công bằng cách có thể lọcc và chặn các yêu cầu bất thường, giúp giảm thiểu lưu lượng tấn công.

3. Load Balancer: Phân phối lưu lượng truy cập giữa các máy chủ (Amazon Elastic Load Balancing (ELB)

4. DDoS Protection Service: Sử dụng dịch vụ chuyên dụng như Cloudflare hoặc AWS Shield để phát hiện và giảm thiểu các cuộc tấn công.

5. Rate Limiting: Giới hạn số lượng yêu cầu từ một IP trong một khoảng limit time.