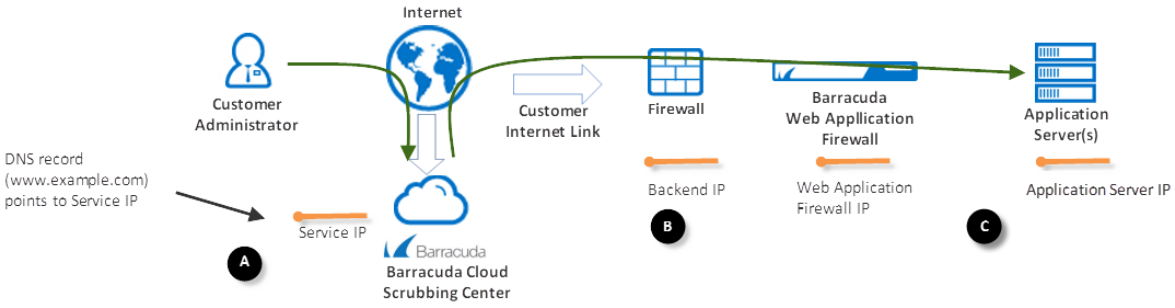
Understanding Service Architecture with Barracuda Active DDoS Prevention

https://campus.barracuda.com/doc/73700725/

When setting up your system to direct traffic to Barracuda Networks, it is helpful to understand the architecture of a service that uses Barracuda Active DDoS Prevention.



The diagram above illustrates the following important points:

A. Barracuda Networks allocates a Service IP to each service. During setup, you will change your DNS record to point all traffic to the Service IP.

B. After Barracuda Networks filters the incoming traffic, it sends your traffic to the Backend IP address. The Backend IP address is the IP address your DNS record would point to if you were not using Barracuda Active DDoS Protection.

- **Typical Backend IP address value**: The virtual IP address defined for this service on your Barracuda Web Application Firewall.
- **Backend IP address value with a network firewall:** If your Barracuda Web Application Firewall is behind a network firewall performing network address translation (NAT), the Backend IP is the address your network firewall forwards to the Web Application Firewall's Virtual IP Address for this service.

C. The Barracuda Web Application Firewall filters web application attacks, then sends traffic to your application servers.

Figures