Setting up Active DDoS Prevention in AWS

https://campus.barracuda.com/doc/79467512/

When you set up Barracuda Active DDoS Prevention, traffic to your application flows first to Barracuda's datacenters for DDoS protection, and then to your Barracuda Web Application Firewall. For more information, see Understanding Service Architecture with Barracuda Active DDoS Prevention.

Deploying in AWS with Clustering or Auto-Scaling

If you deploy your Web Application Firewalls in AWS, and you use either clustering or auto-scaling, you need to put a load balancer in front of your Web Application Firewalls to automatically balance traffic between your Web Application Firewalls. For more information, see Load Balancing For Clustered Barracuda CloudGen WAF Instances in Amazon Web Services (AWS).

Deploying in AWS with an AWS Elastic Load Balancer

When setting up Barracuda Active DDoS Prevention with an AWS Elastic Load Balancer, your configuration must support Source IP Preservation. Source IP Preservation is a feature of the AWS Load Balancer that sends the correct source IP directly to your Barracuda Web Application Firewall. Without Source IP Preservation, your Web Application Firewalls cannot tell which traffic is trusted and which is not, and they will reject all traffic coming from Barracuda Active DDoS Prevention.

To support Source IP Preservation, you must meet these requirements:

- Use a Network Load Balancer. You cannot use a Classic Load Balancer or Application Load Balancer with Barracuda Active DDoS Prevention.
- Ensure that the port of the load balancer's Listener is the same as the port of the Target Group.This will typically be 80 or 443.
- In the load balancer's target group, select targets by Instance ID, not by IP address.This is required to enable Source IP Preservation. See "Source IP Preservation" in this AWS documentation article for more information.

After you have configured the Network Load Balancer, proceed to Setting Up Barracuda Active DDoS Prevention. In Part B of the setup wizard, when prompted for your backend IP address, do not enter the IP address of your Web Application Firewall. Instead, enter the hostname of your Network Load Balancer, a colon, and the port of the Listener you have configured. For example, `test-1c0a2247a964df54.elb.us-west-1.amazonaws.com:443`.