DDoS Protection System for Cloud: Architecture and Tool

Panel No. 06	Batch No. NW000156
Supervisor Name	Shaurya Singh Srinet – RA2111032010006
Dr. Balaji Srikaanth P, AP/NWC	Shounak Chandra – RA2111032010026
Dr. S. Nagendra Prabhu, AP/CINTEL	Charvi Jain – RA2111047010113

Functional Document for User Story 1: Setup AWS Environment for DDoS Protection

1. Introduction

The objective of this user story is to set up the AWS environment for hosting and managing the DDoS protection system. This involves configuring AWS services such as EC2 instances, Auto Scaling, and Load Balancer to ensure the system can automatically scale in response to increased traffic, particularly during DDoS attacks. This infrastructure setup will serve as the foundation for deploying and testing the DDoS detection and mitigation system.

2. Product Goal

The goal is to create a scalable AWS infrastructure to simulate and handle varying traffic loads, including benign and malicious traffic, ensuring that the system is resilient during DDoS attacks. This setup is crucial for testing the performance and effectiveness of DDoS protection mechanisms under real-world conditions.

3. Demography (Users Location)

- **Target Users:** Cloud engineers, security testers, developers working on DDoS protection.
- **User Characteristics:** Technical users with expertise in cloud infrastructure and DDoS mitigation strategies.
- **Location:** Global usage with a focus on cloud environments and organizations requiring DDoS protection.

4. Business Processes

- **AWS Infrastructure Setup:**
  - Configure EC2 instances for running the DDoS protection system.
  - Set up Auto Scaling to manage server capacity during fluctuating traffic.

    - Configure Elastic Load Balancer to distribute traffic evenly among EC2 instances.
- **Traffic Simulation:**
    - Simulate various traffic patterns, including benign and DDoS attacks, to evaluate system performance.
    - Monitor the infrastructure using AWS CloudWatch for traffic metrics and scaling activity.

5. Features

- **EC2 Instance Configuration:**
    - Launch EC2 instances with the necessary configurations (CPU, memory, etc.).
    - Set up security groups and IAM roles for secure access.
- **Auto Scaling Setup:**
    - Configure Auto Scaling policies to scale instances based on CPU usage or incoming traffic.
    - Ensure the system can scale up and down based on defined thresholds.
- **Elastic Load Balancer:**
    - Set up the Elastic Load Balancer (ELB) to distribute traffic among EC2 instances.
    - Ensure the load balancer is properly configured to handle both normal and attack traffic.
- **SSH Connectivity:**
    - Establish SSH access for remote management and troubleshooting of EC2 instances.

6. Authorization Matrix

ROLE	**Access Level**
Developer	Full access to configure and manage AWS resources.
Security Tester	Access to traffic logs and performance metrics.
Admin	Full access to AWS environment and all configurations.

7. Assumptions

- AWS environment is stable, and resources are available.
- Proper AWS IAM roles and permissions are configured for each user.
- Sufficient network bandwidth is available for testing traffic simulations.
- Security groups and access control lists are set up to restrict access as needed

8. Target Audience

- **Audience:** Cloud engineers, system architects, security teams, and developers working on DDoS protection systems.
- **Effort Estimation:** Approximately 5 days to 1 week for setup and testing, depending on complexity and available resources.

9. Acceptance Criteria

- AWS EC2 instances are set up and accessible.
- Auto Scaling is configured to automatically scale the system based on incoming traffic.
- Load Balancer is properly distributing traffic among EC2 instances.
- SSH access to EC2 instances is tested and verified.
- The infrastructure setup is documented and includes steps for scaling, troubleshooting, and monitoring.

10. Checklist

- EC2 instances are launched and configured.
- Auto Scaling policies are defined and tested.
- Elastic Load Balancer is set up and routing traffic correctly.
- SSH connectivity is established and verified.
- The setup is documented, including troubleshooting steps and scaling guidelines.