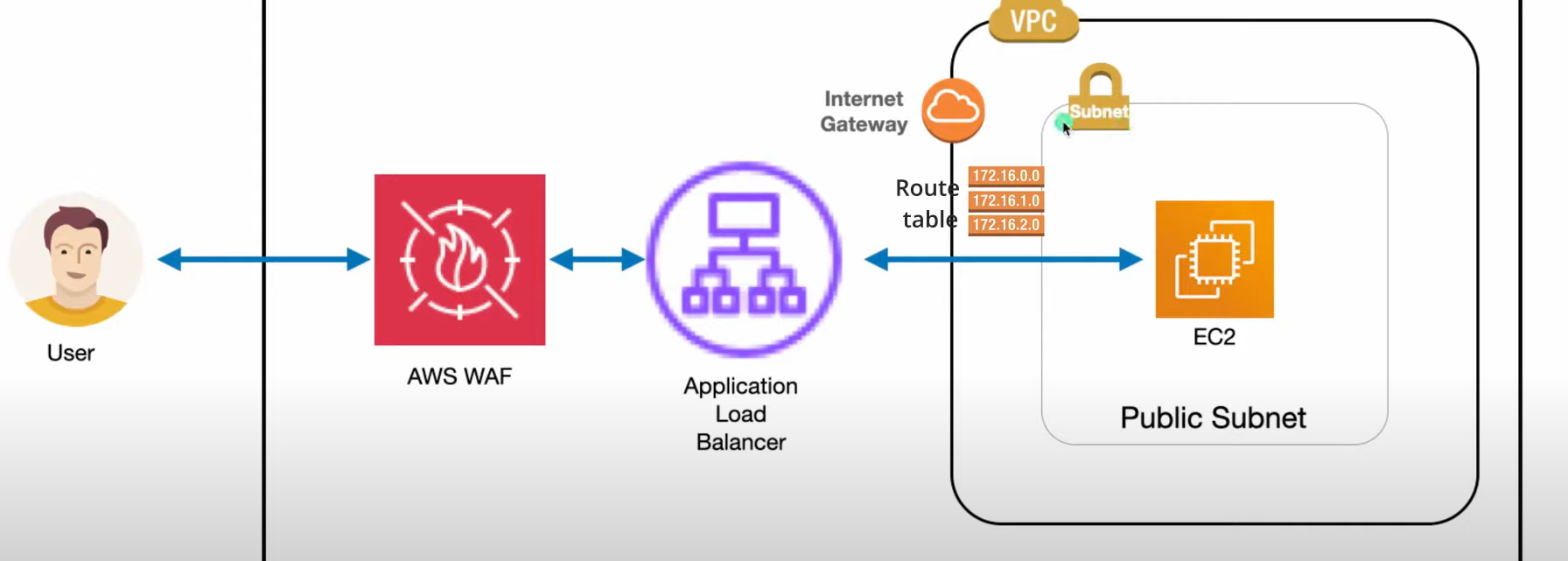
Project Summary: Secure Web Application Deployment with AWS WAF

AWS WAF (Web Application Firewall) is a security service that helps protect web applications from common threats and vulnerabilities, such as SQL injection, cross-site scripting (XSS), and other web exploits that could affect availability, compromise security, or consume excessive resources.



STEP!:-**1. Create a VPC**

1. Navigate to **VPC Dashboard** → **Your VPCs** → **Create VPC**.
2. Configure the VPC:
   * **Name tag**: MY-VPC-for-waf.
   * **IPv4 CIDR block**: 12.0.0.0/16.
3. Click **Create VPC**.

**2. Create Two Public Subnets**

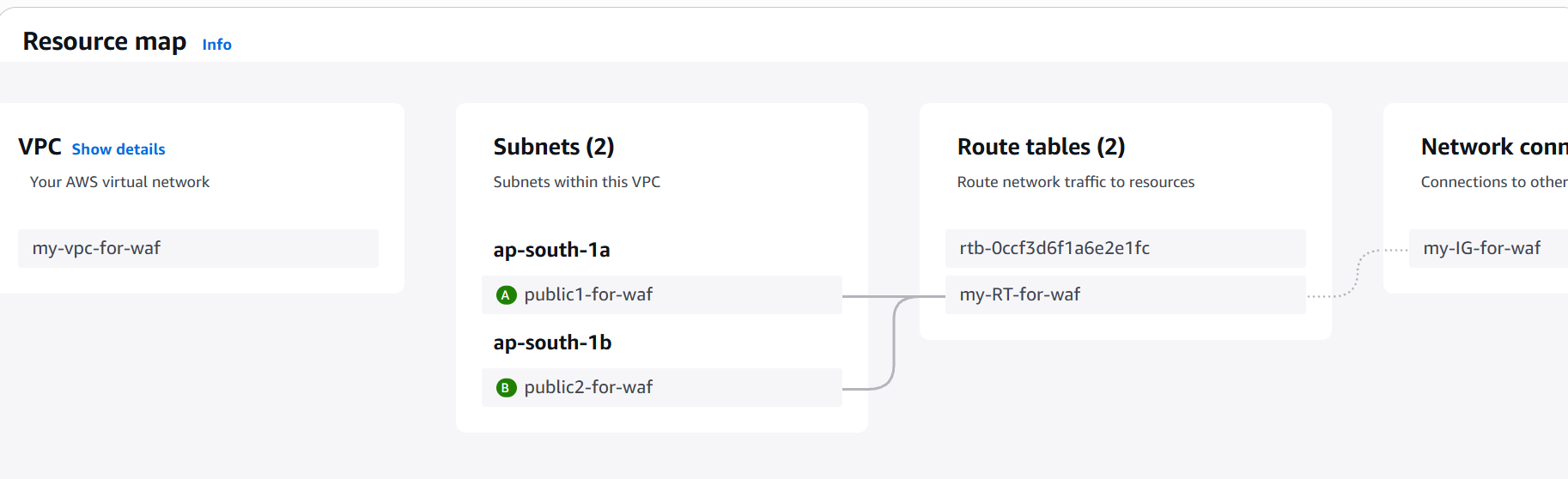
1. Navigate to **Subnets** → **Create Subnet**.
2. Create the subnets:
   * **Subnet Name**: public1.
     + **VPC**: MY-VPC-for-waf.
     + **CIDR Block**: 12.0.1.0/24.
   * **Subnet Name**: public2.
     + **VPC**: MY-VPC-for-waf.
     + **CIDR Block**: 12.0.2.0/24.
3. Mark both subnets as public:
   * Select each subnet → **Actions** → **Modify Auto-Assign IP Settings**.
   * Enable **Auto-assign public IPv4 address**.
4. Save changes.

**3. Create an Internet Gateway**

1. Navigate to **Internet Gateways** → **Create Internet Gateway**.
   * **Name tag**: MY-IG-for-waf.
2. Attach the Internet Gateway:
   * Select the created Internet Gateway → **Actions** → **Attach to VPC**.
   * Select MY-VPC-for-waf.

**4. Create a Route Table**

1. Navigate to **Route Tables** → **Create Route Table**.
   * **Name tag**: MY-RT-for-waf.
   * **VPC**: MY-VPC-for-waf.
2. Add a route to the Internet Gateway:
   * Select the route table → **Routes** → **Edit Routes** → **Add Route**.
     + **Destination**: 0.0.0.0/0.
     + **Target**: MY-IG-for-waf.
   * Save the route.
3. Associate the route table with both public subnets:
   * Select the route table → **Subnet Associations** → **Edit Subnet Associations**.
   * Select public1 and public2.



**5. Launch an EC2 Instance**

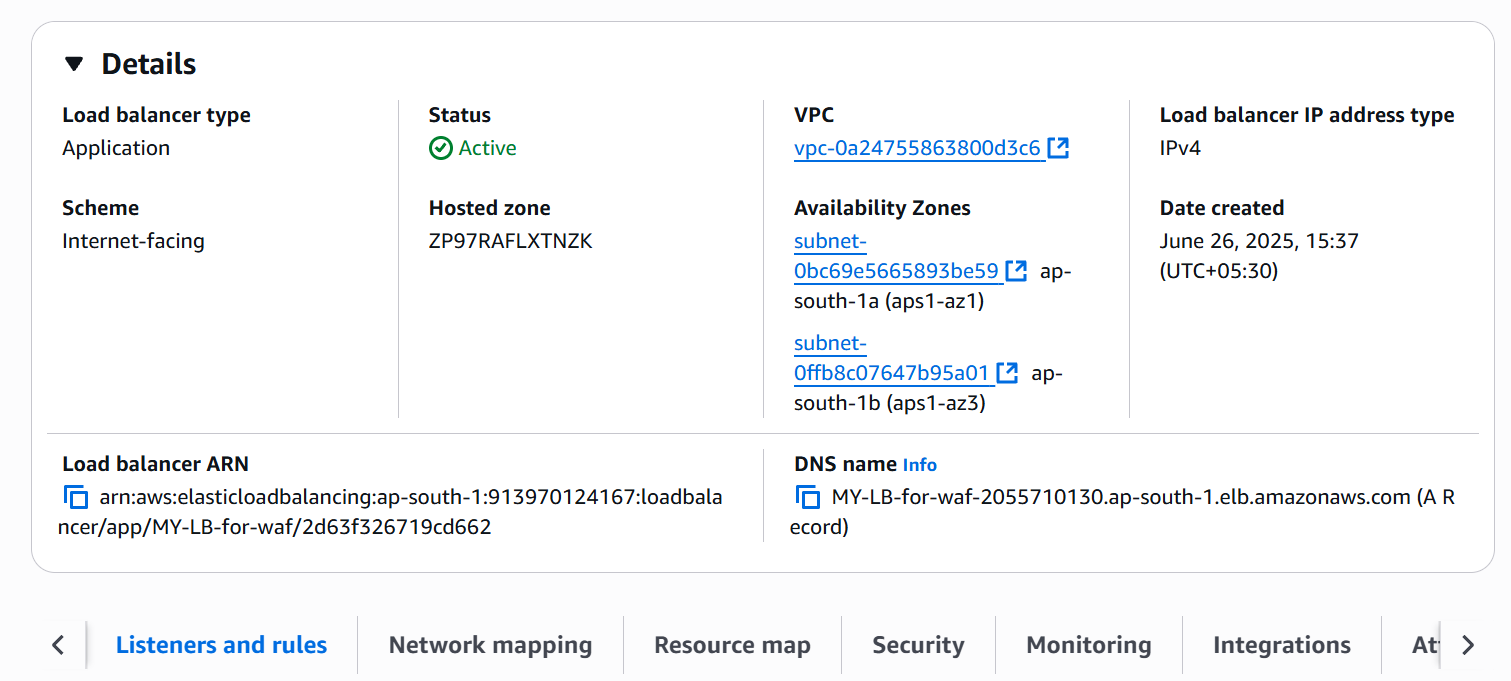
1. Navigate to **EC2 Dashboard** → **Launch Instance**.
2. Configure the instance:
   * **Name**: Choose any name.
   * **AMI**: Amazon Linux 2 (or your preferred AMI).
   * **Instance type**: e.g., t2.micro.
   * **Key Pair**: Select or create a key pair.
   * **Network Settings**:
     + **VPC**: MY-VPC-for-waf.
     + **Subnet**: public1.
     + **Auto-assign Public IP**: Enabled.
   * **Security Group**:
     + **Name**: MY-SG-for-waf.
     + Add the following inbound rules:
       - HTTP (80), HTTPS (443), and SSH (22) from 0.0.0.0/0.
3. Launch the instance.

A screenshot of a computer

AI-generated content may be incorrect.

**6. Create an Application Load Balancer**

1. Navigate to **Load Balancers** → **Create Load Balancer**.
2. Configure the ALB:
   * **Name**: MY-LB-for-waf.
   * **Scheme**: Internet-facing.
   * **VPC**: MY-VPC-for-waf.
   * **Subnets**: Select public1 and public2.
3. Configure the Security Group:
   * Use MY-SG-for-waf.
   * Add the following inbound rules if not already added:
     + HTTP (80) and HTTPS (443) from 0.0.0.0/0.
4. Configure the Target Group:
   * **Name**: MY-TG-for-waf.
   * **Target type**: Instance.
   * **Protocol**: HTTP.
   * Register the EC2 instance created in Step 5.
5. Create the Load Balancer.



A screenshot of a computer

AI-generated content may be incorrect.

**7. Create an AWS WAF ACL and IP Set**

1. Navigate to **WAF & Shield** → **Create web ACL**.
2. Configure the ACL:
   * **Name**: Choose a descriptive name.
   * **Scope**: Regional.
   * **Associated Resource**: MY-LB-for-waf.
3. Add an IP Set:
   * Go to **IP sets** → **Create IP set**.
   * **Name**: Choose a name (e.g., allowed-ips or blocked-ips).
   * **IP version**: IPv4.
   * Add the IP addresses to include in the set.
4. Add a rule to the ACL:
   * Add a **Rule** that uses the IP set.
   * Specify whether the IPs should be allowed or blocked.
5. Save and deploy the ACL.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.