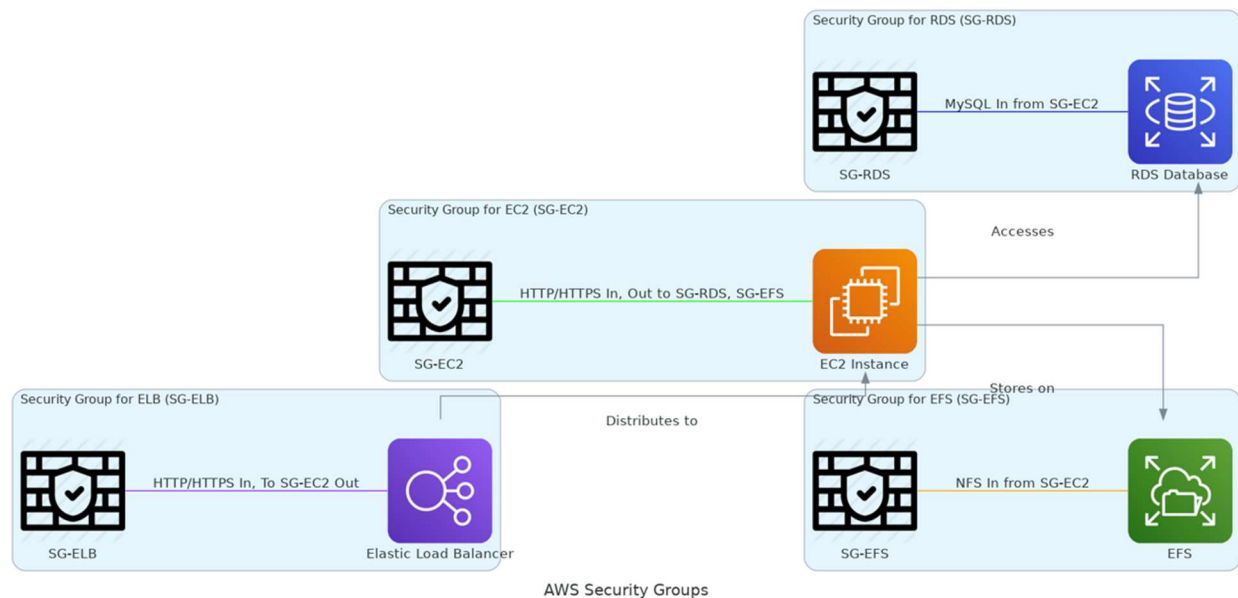


Security groups for my HA WordPress Blog



1. EC2 Instance Security Group (SG-EC2):

- **Assigned to:** EC2 instances hosting your WordPress website.
- **Inbound Rules:**
 - HTTP (port 80) and HTTPS (port 443) from the ELB security group. This restricts web traffic to only come through the load balancer, enhancing security by not exposing the EC2 instances directly to the internet.
- **Outbound Rules:**
 - Allow all traffic to the internet. This enables the EC2 instances to access external resources, if necessary, like updates or APIs.

2. Elastic Load Balancer Security Group (SG-ELB):

- **Assigned to:** Application Load Balancer (ALB).
- **Inbound Rules:**
 - HTTP and HTTPS from anywhere (0.0.0.0/0). This allows the ALB to receive web traffic from any user on the internet.
- **Outbound Rules:**
 - Allow all traffic to the SG-EC2 security group. This ensures that the ALB can forward traffic to the EC2 instances.

3. RDS Security Group (SG-RDS):

- **Assigned to:** RDS database instances.

- **Inbound Rules:**

- Database port (e.g., MySQL port 3306) from SG-EC2. This ensures that only your EC2 instances can access the RDS database, which enhances security by preventing external access.

- **Outbound Rules:**

- Minimal or no specific rules required, as RDS typically doesn't initiate outbound traffic.

4. **EFS Security Group (SG-EFS):**

- **Assigned to:** EFS File System.

- **Inbound Rules:**

- NFS (port 2049) from SG-EC2. This allows the EC2 instances to access the EFS file system for shared storage.

- **Outbound Rules:**

- Typically, outbound rules are not required for EFS, as it does not initiate connections but only responds to requests from authorized instances.