**Security Groups**

Security Groups act as virtual firewalls for your EC2 instances. They control the inbound and outbound traffic to ensure your instances are secure.

**Key Points**

* **Inbound Rules**: Specify the allowed incoming traffic. Example rules include:
  + Allow HTTP (port 80) from anywhere.
  + Allow SSH (port 22) only from specific IP addresses.
* **Outbound Rules**: Define the allowed outgoing traffic. By default, all outbound traffic is allowed.

**Best Practices**

* **Least Privilege**: Only open the necessary ports and restrict access to specific IP ranges or security groups.
* **Regular Review**: Periodically review security group rules to ensure they adhere to current security policies.

**Example Configuration**

* **Web Server**: Allow HTTP (port 80) and HTTPS (port 443) from any IP address.
* **Database**: Restrict access to the database instance by allowing connections only from specific IP addresses or security groups.

**Certification Tips**

* **Understand security group configurations and best practices**: Important for AWS Certified Solutions Architect and AWS Certified Security Specialty exams.

**Resources**

* [Security Groups for Your VPC](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html)
* [Best Practices for Security Groups](https://aws.amazon.com/answers/security/security-groups/)