AWS EC2 Security Group Update - SOP

Standard Operating Procedure (SOP) Document

1. Document Control
- Document Title: AWS EC2 Security Group Update
- Document Owner: [Name/Role]
- Prepared By: [Name/Role]
- Approved By: [Name/Role]
- Version: 1.0
- Last Updated: [Date]

2. Overview
AWS EC2 Security Group Update - Standard Operating Procedure (SOP) Overview
This SOP outlines the process to add inbound rules for ports 22 (SSH) and 443 (HTTPS)
to an AWS EC2 instance security group, allowing secure administrative access and web traffic.
- Platform: AWS
- Code Language: AWS CLI / Python (Optional for automation)

Required Dependencies
- AWS CLI installed
- boto3 (Python SDK for AWS)

Credentials Required
- AWS_ACCESS_KEY_ID
- AWS_SECRET_ACCESS_KEY
- AWS_REGION
- IAM user with EC2 Security Group modification permissions

3. Input Parameters
1. instance_id
- Type: string
- Description: Unique identifier for the EC2 instance whose security group will be updated.
- Required: true
- Default: null

2. security_group_id
- Type: string

- Description: ID of the security group associated with the EC2 instance.
- Required: true
- Default: null

3. cidr_range
- Type: string
- Description: CIDR block specifying the IP range allowed to access the instance.
- Required: true
- Default: 0.0.0.0/0
- Example: 192.168.1.0/24

4. region
- Type: string
- Description: AWS region where the instance is deployed.
- Required: true
- Default: null
- Example Values: us-east-1, eu-west-1

4. Logic Flow
1. Pre-Creation Validation
- Validate AWS credentials and permissions.
- Verify the instance ID and security group exist.
- Ensure the CIDR range is correct and follows best practices.

2. Rule Addition Process
- Identify the security group associated with the EC2 instance.
- Add inbound rules for the following:
  * Port 22 (SSH) ? Allows remote administrative access.
  * Port 443 (HTTPS) ? Allows secure web traffic.
- Apply rules using AWS CLI or boto3.

3. Post-Creation Configuration
- Validate that the rules are applied successfully.
- Describe the security group and ensure ports 22 and 443 appear under inbound rules.
- Test SSH and HTTPS connections to confirm accessibility.

5. Error Handling Scenarios

- Security group not found or invalid.
- CIDR block incorrectly formatted.
- Insufficient IAM permissions to modify security groups.
- Conflicting rules or network ACLs blocking traffic.

6. Success Criteria

- Ports 22 and 443 are open and accessible.
- Inbound rules reflect the specified CIDR block.
- SSH and HTTPS traffic can reach the EC2 instance.

7. Monitoring Considerations

- Regularly audit security group rules.
- Use AWS CloudTrail to track security group modifications.
- Restrict CIDR blocks to reduce exposure to global IP traffic.

8. Notes and Considerations

- Opening 0.0.0.0/0 increases the risk of malicious activity.
- Regularly review security group rules to align with AWS best practices.
- For enhanced security, consider allowing access only from trusted IPs.

9. Change Management

- All modifications to the Security Group update process must be approved by authorized personnel.
- Update the SOP if any new best practices or requirements are introduced.

10. References

- AWS Documentation - Security Groups: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html
- Organizational Cloud Security Policy: [Internal Link or Document Reference]