AWS EC2 Security Group Update

Enable Inbound Rules for Ports 22 (SSH) and 443 (HTTPS)

1. Overview

This document outlines the procedure to add inbound rules for ports 22 (SSH) and 443 (HTTPS) to the security group of an AWS EC2 instance. These rules allow remote SSH access and HTTPS traffic to the instance.

2. Purpose

The purpose of this process is to ensure that the instance is accessible for administrative tasks (port 22) and secure web traffic (port 443). This is essential for instances hosting web applications or requiring secure remote management.

3. Pre-requisites

- AWS CLI installed and configured with necessary permissions.
- IAM user with EC2 security group modification permissions.
- Instance ID of the target EC2 instance.
- Access to the AWS Management Console or CLI.

4. Required Parameters

- Instance ID: The EC2 instance to which the rules will be applied.
- Security Group ID: The security group associated with the instance.
- CIDR Range: 0.0.0.0/0 for open access or a specific IP range.
- AWS Region: Region where the instance is deployed.

AWS EC2 Security Group Update

Enable Inbound Rules for Ports 22 (SSH) and 443 (HTTPS)

5. Process Overview

1. Identify the security group associated with the EC2 instance.

2. Add inbound rules to the security group for:

   - Port 22 (SSH) - Allow remote access.

   - Port 443 (HTTPS) - Allow secure web traffic.

3. Validate rule application using the AWS CLI or Management Console.

4. Document the changes for compliance and audit purposes.

6. Verification and Validation

After applying the rules, verify their existence by describing the security group:

1. Use the AWS CLI to describe the security group.

2. Ensure ports 22 and 443 are listed under inbound rules.

3. Test SSH and HTTPS access to confirm the rules are active.

7. Troubleshooting

1. If inbound traffic is still blocked, ensure no conflicting deny rules exist.

2. Check for overlapping rules or misconfigured network ACLs.

3. Review AWS CloudTrail logs to track changes in the security group.

4. Ensure the correct CIDR block is used (e.g., 0.0.0.0/0 for global access).

8. Notes and Considerations

AWS EC2 Security Group Update

Enable Inbound Rules for Ports 22 (SSH) and 443 (HTTPS)

- Allowing 0.0.0.0/0 opens the instance to all IP addresses, increasing risk. Restrict access by using specific IP addresses or IP ranges.
- Regularly audit security group rules to ensure compliance with security best practices.