**SOP for Security Groups to restrict traffic within the Amazon VPC**

**Objective:** This SOP provides guidelines and procedures to ensure the security of the Virtual Private Cloud (Amazon VPC) and secure traffic within the VPC by implementing security groups

**Scope:** This SOP applies to all AWS accounts and personnel responsible for managing and securing Amazon VPCs.

|  |  |
| --- | --- |
| **Roles** | **Responsibilities** |
| AWS Account Owner | Responsible for managing the overall security of Amazon VPCs. |
| AWS VPC Administrator | Responsible for implementing and maintaining security groups and network ACLs within Amazon VPCs. |
| Network Security Team | Responsible for reviewing and approving security configurations and conducting periodic audits. |

**Procedure:**

**Security Groups to restrict traffic within the Amazon VPC**

* Create security groups to restrict traffic between resources within the Amazon VPC: <https://docs.aws.amazon.com/vpc/latest/userguide/security-groups.html>
* Define security group rules to allow only necessary communication between resources:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html>

* Limit access to specific ports, protocols, and IP ranges based on the resource requirements.

<https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html>

* Regularly review and update security group rules to maintain least privilege access:

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

* Document the security group configurations, including rules, allowed ports, and associated resources.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules.html>