**SOP for Network ACLs to Restrict Inbound and Outbound Traffic**

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

**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. |

**Network ACLs to Restrict Inbound and Outbound Traffic:**

Implement network ACLs to control inbound and outbound traffic at the subnet level.

[https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#custom-network-acl](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html%23custom-network-acl)

Define appropriate rules to allow or deny specific IP addresses, ports, and protocols.

[https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#CreateACL](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html%23CreateACL)

Follow the principle of least privilege by allowing only necessary traffic and blocking unauthorized access.

[https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html#elb-vpc-nacl](https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html%23elb-vpc-nacl)

Regularly review and update network ACL rules to align with security requirements.

[https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html#ACLSubnet](https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html%23ACLSubnet)

Document the network ACL configurations, including rules, allowed traffic, and associated subnets.

**Network ACL rules**

You can add or remove rules from the default network ACL, or create additional network ACLs for your VPC. When you add or remove rules from a network ACL, the changes are automatically applied to the subnets that it's associated with.

The following are the parts of a network ACL rule:

* **Rule number**. Rules are evaluated starting with the lowest numbered rule. As soon as a rule matches traffic, it's applied regardless of any higher-numbered rule that might contradict it.
* **Type**. The type of traffic; for example, SSH. You can also specify all traffic or a custom range.
* **Protocol**. You can specify any protocol that has a standard protocol number. For more information, see [Protocol Numbers](http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml). If you specify ICMP as the protocol, you can specify any or all of the ICMP types and codes.
* **Port range**. The listening port or port range for the traffic. For example, 80 for HTTP traffic.
* **Source**. [Inbound rules only] The source of the traffic (CIDR range).
* **Destination**. [Outbound rules only] The destination for the traffic (CIDR range).
* **Allow/Deny**. Whether to *allow* or *deny* the specified traffic.

If you add a rule using a command line tool or the Amazon EC2 API, the CIDR range is automatically modified to its canonical form. For example, if you specify 100.68.0.18/18 for the CIDR range, we create a rule with a 100.68.0.0/18 CIDR range.