Access Control Measures Implementation Report

Objective

This report outlines the implementation of access control measures, including one Access Control List (ACL) configuration, one access control model, and one user access level.

1. Access Control List (ACL) Configuration

Description

An Access Control List (ACL) is implemented to restrict traffic to a server, allowing access only from specific trusted IP addresses.

ACL Rule Example

- Permit traffic from IP range 192.168.1.0/24 to server 192.168.1.10 on port 80.
- Deny all other traffic.
- This ensures that only devices within the trusted internal network can access the server.

Configuration

For example, in Cisco router configuration:

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 192.168.1.10 eq 80
access-list 100 deny ip any any
```

Purpose

The ACL prevents unauthorized access to critical resources, allowing traffic only from trusted sources.

2. Access Control Model

Description

The Discretionary Access Control (DAC) model is implemented to allow resource owners to determine access permissions.

Implementation

For example, in a file system:

- User A owns a file (data.txt) and grants read access to User B.

```
  chmod 640 data.txt
```

- Only User A can modify permissions or content of the file.

Purpose

DAC provides flexibility by allowing resource owners to determine who can access their resources.

3. User Access Level

Description

A user access level defines the permissions granted to a user within a system. For example, in a database management system, users are assigned roles with specific access rights.

Example

Role: Database Viewer

- Permissions: Read-only access to specific tables (e.g., employees and salaries).
- Command: GRANT SELECT ON employees, salaries TO 'viewer_user';
- This ensures the user can view data but cannot modify it.

Purpose

User access levels enforce the principle of least privilege, limiting users to only the access necessary for their roles.

Conclusion

The implementation of ACLs, access control models, and user access levels creates a secure and manageable system. These measures ensure that resources are accessed appropriately and unauthorized access is prevented.