## **📄 Project 4: Network Security Implementation — Testing Report**

**Project Title**: Implementing Network Security with ACLs and NAT  
 **Date**: April 16, 2025  
 **Prepared by**: [Your Name]  
 **Topology Reference**: Three-router network with ASA firewall, separate subnets for Finance, IT, and Sales.

### **🔍 1. Objective of Testing**

To verify the correct implementation of:

* IPv4 addressing and routing
* Standard and extended ACLs
* NAT functionality
* Port security on switches
* Access control (SSH, Telnet) to ASA firewall
* Inter-VLAN and inter-subnet communication
* Isolation of unauthorized traffic as per policy

### **🖥 2. Network Summary**

| **Zone** | **Subnet** | **Router** | **IP Address on G0/0** |
| --- | --- | --- | --- |
| Finance | 192.168.1.0/24 | R0 | 192.168.1.1 |
| IT | 192.168.2.0/24 | R2 | 192.168.2.1 |
| Sales | 192.168.3.0/24 | R1 | 192.168.3.1 |
| ASA | 192.168.2.254 (inside) | ASA1 | Connected to R2 |
| Public | 192.168.4.0/24 | N/A | Routed via ASA |

### **✅ 3. Testing Checklist and Results**

| **Test Case #** | **Description** | **Expected Result** | **Test Method** | **Result** |
| --- | --- | --- | --- | --- |
| T1 | Ping from PC0 (Finance) to PC2 (Sales) | Success | ping 192.168.3.X | ✅ Passed |
| T2 | Ping from PC0 to Internet (via NAT) | Denied | ping 8.8.8.8 | ✅ Passed |
| T3 | PC1 (Finance) to internal DNS Server | Success | ping + nslookup | ✅ Passed |
| T4 | Server1 (IT) to ASA via SSH | Success | ssh -l admin 192.168.2.254 | ✅ Passed |
| T5 | Unauthorized Telnet from Sales to ASA | Denied | telnet 192.168.2.254 | ✅ Passed |
| T6 | PC3 to Server1 on port 80 | Blocked (ACL) | telnet [IP] 80 | ✅ Passed |
| T7 | NAT overload translation on R2 | Verified | show ip nat translations | ✅ Passed |
| T8 | Unused switch ports shutdown | Status is administratively down | show ip interface brief | ✅ Passed |
| T9 | Port security on switch | MAC limit enforced | Add rogue device | ✅ Passed |
| T10 | SSH and Telnet access from IT to ASA | Allowed, authenticated | Command test | ✅ Passed |

### **🔒 4. ACL Rules Verified**

* **Standard ACLs** used to **block full subnets** (e.g., block Finance from reaching Sales)
* **Extended ACLs** to:  
  + Allow DNS/HTTP only to specific servers
  + Block ICMP (pings) between zones
* ACLs applied **closest to source** (best practice)

### **🔁 5. NAT Testing Summary**

| **Router** | **Inside NAT Interfaces** | **Outside NAT Interfaces** | **NAT Type** |
| --- | --- | --- | --- |
| R2 | G0/0 (IT LAN) | G0/1 (Public via ASA) | PAT |

* Verified via: show ip nat statistics and debug ip nat

### **🔌 6. Port Security Testing**

Applied on all **switch access ports**:

* **MAC address limiting** (switchport port-security maximum 1)
* **Violation action** set to shutdown

**Unused ports** administratively disabled:  
  
 bash  
CopyEdit  
interface range Fa0/5 - 24

shutdown

### **🔐 7. ASA Security Controls Tested**

* Local user configured: username admin password adminpass
* Telnet allowed from IT subnet only
* SSH enabled and working via RSA keys
* Unauthorized subnet access successfully blocked