Security & ACLs Playbook

# 1. Purpose

The purpose of this step is to implement layered security controls that protect the network while enforcing business policies. Security features ensure that only authorized devices and users have access, inter-VLAN traffic is properly segmented, and management access remains secure. ACLs provide policy enforcement, while NAT ensures inside devices can still reach external resources securely. Together, these steps simulate real-world enterprise security practices within the project environment.

# 2. Security & ACLs – Playbook

## Step 1: Secure Management Access

- Configure SSH-only access on routers and switches.  
- Disable unused services (e.g., Telnet, HTTP).  
  
line vty 0 4  
 transport input ssh  
 login local  
exit  
service password-encryption  
  
Verify with: show running-config | include vty

## Step 2: Port Security on Switches

- Apply port-security on all access ports.  
- Limit max MAC addresses per port.  
- Set violation mode (restrict or shutdown).  
  
interface fa0/5  
 switchport mode access  
 switchport access vlan 20  
 switchport port-security  
 switchport port-security maximum 2  
 switchport port-security violation restrict  
 switchport port-security mac-address sticky  
  
Verify with: show port-security interface fa0/5

## Step 3: VLAN99 (Holding VLAN)

- Move unused ports into VLAN99.  
- Shut them down to prevent rogue devices.  
  
interface range fa0/9 - 24  
 switchport mode access  
 switchport access vlan 99  
 shutdown  
  
Verify with: show vlan brief

## Step 4: Inter-VLAN Access Control Lists (ACLs)

- Define an extended ACL to enforce project policies:  
 • Deny Sales ↔ Engineering communication.  
 • Allow Management full access.  
 • Allow all VLANs Internet access.  
  
ip access-list extended VLAN-POLICY  
 deny ip 192.168.99.16 0.0.0.15 192.168.99.32 0.0.0.15  
 deny ip 192.168.99.32 0.0.0.15 192.168.99.16 0.0.0.15  
 permit ip 192.168.99.0 0.0.0.15 any  
 permit ip 192.168.99.0 0.0.0.127 any  
  
Apply ACL inbound on VLAN subinterfaces:  
interface fa0/0.10  
 ip access-group VLAN-POLICY in  
interface fa0/0.20  
 ip access-group VLAN-POLICY in  
interface fa0/0.30  
 ip access-group VLAN-POLICY in  
interface fa0/0.99  
 ip access-group VLAN-POLICY in  
  
Verify with: show access-lists

## Step 5: NAT Overload (HQ-RTR)

- Ensure inside networks can still reach the ISP:  
  
access-list 10 permit 192.168.99.0 0.0.0.127  
ip nat inside source list 10 interface fa0/1 overload  
  
Verify with: show ip nat translations

# 3. Explanation

These steps implement layered security: SSH-only access ensures management sessions are encrypted, port security prevents unauthorized devices from hijacking switch ports, and VLAN99 isolates/shuts down unused ports to reduce the attack surface. ACLs enforce business rules by blocking Sales and Engineering VLANs from directly communicating, while allowing Management oversight and Internet access for all. NAT Overload allows internal devices to share a single public IP while hiding private addresses. Combined, these measures create a secure, policy-compliant, and realistic enterprise network.