**Firewall, Security Group & VPC Setup Confirmation**

**Project:** Telco Cloud Migration & Enablement  
**Environment:** [e.g., AWS Production / OpenStack Staging / GCP UAT]  
**Date:** [Insert Date]  
**Prepared by:** [Name, Role, Organization]

**1. Executive Summary**

This document confirms the completion and verification of all firewall rules, security groups, and Virtual Private Cloud (VPC) configurations as per network architecture and security policies for the Telco Cloud migration project. These setups are crucial to ensuring secured interconnectivity between components such as CRM, OSS/BSS, NFV stack, and third-party integrations (e.g., M-PESA APIs).

**2. VPC Configuration Overview**

| **Parameter** | **Value** |
| --- | --- |
| VPC ID | vpc-xxxxxxxx |
| CIDR Range | 10.0.0.0/16 |
| Region / Zone | [e.g., us-east-1a] |
| Subnets Created | Public (10.0.1.0/24), Private (10.0.2.0/24) |
| NAT Gateway | Configured for private subnet |
| VPN/Direct Connect Tunnel | Established to Telco on-prem |

**3. Security Group Setup**

| **Security Group Name** | **Inbound Rules (Port/Protocol)** | **Source/Destination** | **Purpose** |
| --- | --- | --- | --- |
| crm-sg | TCP 443 (HTTPS) | M-PESA Public IP | Enable secure M-PESA API access |
| oss-internal | TCP 22, 8080 | 10.0.0.0/16 | Admin and OSS web interface access |
| nfv-cluster | TCP 6443, 10250–10255 | K8s worker nodes | Kubernetes API & agent communication |
| bss-database-sg | TCP 3306 | OSS/BSS VMs only | MySQL DB for BSS module |

**4. Firewall Rules (Cloud Provider / On-Prem Edge Firewall)**

| **Rule ID** | **Direction** | **Port Range** | **Protocol** | **Source** | **Destination** | **Status** |
| --- | --- | --- | --- | --- | --- | --- |
| FW-001 | Ingress | 443 | TCP | 41.90.x.x (M-PESA) | 10.0.2.5 (CRM) | ✅ Active |
| FW-002 | Egress | 53 | UDP | 10.0.1.10 | Public DNS | ✅ Active |
| FW-003 | Ingress | 22 | TCP | Admin JumpBox IP only | All Instances | ✅ Restricted |
| FW-004 | Ingress | 8443 | TCP | 10.0.2.0/24 | NFV Controller | ✅ Verified |

**5. Peering / Routing Configuration**

* **VPC Peering:** Established between OSS subnet and NFV subnet
* **Route Tables Updated:** Confirmed propagation of M-PESA IP range through NAT Gateway
* **DNS Resolver Forwarding:** Configured for internal service discovery between BSS and CRM

**6. Testing and Validation Summary**

| **Test** | **Result** | **Performed By** | **Date** | **Comments** |
| --- | --- | --- | --- | --- |
| Ping from OSS to M-PESA Gateway | Success | NetOps | [Date] | No latency beyond 50ms |
| HTTPS request to CRM via SG | Success | DevOps | [Date] | TLS 1.2 handshake verified |
| Database port lock on BSS DB | Success | SecOps | [Date] | Unreachable from unauthorized IPs |
| Kubernetes Master API access | Success | Cloud Engineer | [Date] | RBAC enforced at kube-apiserver level |

**7. Attachments (if applicable)**

* Network Topology Diagram (VPC + Firewall + Peering)
* Cloud Firewall Export (CSV/JSON)
* Security Group Snapshots
* Test Logs and Ping Results

**8. Sign-off**

**Confirmed By (Cloud/Network Lead):**  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Reviewed By (Security Lead):**  
Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_