

TERMS OF REFERENCE

Position:	Network Engineer
Rank / Classification:	Lead
Division	Technology, Product and Innovation Division
Duration / Post Type:	Permanent/ Full Time
Reporting Line:	Chief Technology Officer (CTO)

1. Background & Scope

The Network Engineer is responsible for designing, operating, securing, and continuously improving the organisation's LAN, WAN, data centre, and perimeter network infrastructure. The core scope encompasses managing L2/L3 routing and switching across primary and DR sites, maintaining strict PCI-DSS Cardholder Data Environment (CDE) segmentation, administering next-generation firewalls and partner IPsec/cloud interconnects, optimizing core services (DNS, DHCP, load balancing), and automating device configurations—all while ensuring high availability, continuous patch currency, and strict compliance with PCI-DSS, ISO 27001, and regulatory standards.

2. Key Responsibilities

- **Core & Data Centre Network Operations:** Manage L2/L3 infrastructure, BGP/OSPF routing, VLANs, VRFs, first-hop redundancy (HSRP/VRRP), QoS policies, and out-of-band management.
- **Perimeter Security & Firewall Governance:** Administer next-generation firewalls, execute six-monthly rule reviews, tune IDS/IPS and DDoS controls, and forward logs to SIEM.
- **Network Segmentation & Compliance:** Maintain CDE segmentation, cardholder data-flow diagrams, bastion hosts, and support annual penetration testing and ASV scans.
- **WAN, Interconnects & Cloud Connectivity:** Oversee MPLS/broadband circuits, partner IPsec VPNs, AWS Direct Connect/Transit Gateway hybrid networking, and remote-access VPNs.
- **Load Balancing & Core Services:** Configure load balancers (HAProxy/F5), internal/external DNS, DHCP scopes, NTP synchronization, and TLS certificate lifecycles.
- **Monitoring, Automation & Change Control:** Operate monitoring platforms (Zabbix/NetFlow), lead packet-level troubleshooting, automate device backups/version control and Ansible/Python (Netmiko) scripts, enforce CAB change management, apply CIS golden baselines, centralise TACACS+/RADIUS AAA, oversee firmware patch lifecycles, and maintain complete network documentation, SOPs, and runbooks

3. Qualifications & Experience

- Bachelor's degree in computer science, Information Technology, Network Engineering, Telecommunications, or a related field.
- Relevant vendor certifications (CCNA/CCNP, Fortinet NSE, Palo Alto PCNSA/PCNSE, AWS Networking, ITIL) will be a distinct advantage.
- Minimum 3 years of hands-on experience in enterprise or data centre network engineering.
- Demonstrated expertise in multi-vendor routing/switching (BGP/OSPF), firewalls, IPsec VPNs, load balancing, and network automation (Python/Ansible).
- Prior experience in PCI-DSS segmentation, banking, fintech, or regulated payment environments is highly advantageous.

4. Deliverables

- **Strategic Assessments & Architecture:** Network Estate Gap Analysis Report, Documented PCI-DSS CDE Segmentation Design, and Current Logical/Physical Network Topology & IP Schema.
- **Security & Compliance Baselines:** Firewall & Router Rule-Set Audit Report, Network Device Hardening Baseline with Centralized TACACS+/RADIUS, and PCI-DSS/ISO 27001 Audit Evidence Packages.
- **Operational Frameworks & Observability:** Production Network Monitoring & Alerting Platform, Automated Device Configuration Backup & Version Control Framework, and Network SOPs/Runbooks.
- **Continuity & Capacity Reports:** ISP, WAN & DR Network Failover Test Reports, and Quarterly Network Capacity & Performance Reports.

Specific deliverables and timelines may be determined through annual or periodic work plans approved by the CTO.