OLUWASEYI PAUL BABALOLA

Hamilton, NJ 08610
+1 (609) 960-6148 | babalolaseyip@gmail.com | Project Portfolio | LinkedIn
Authorized to work in the U.S. (Green Card)

SUMMARY

Sr. Network and Cyber Security Engineer with 9+ years of experience designing, securing, and operating large-scale enterprise, data center, and cloud network infrastructures. Proven expertise in network security architecture, firewall platforms, zero-trust access, SD-WAN, and hybrid cloud connectivity across AWS, Azure, and GCP. Highly skilled in multi-vendor security solutions (Palo Alto, Fortinet, Cisco, Check Point, Zscaler) with a strong background in high-availability design, segmentation, security operations, incident response, and compliance-driven environments. Adept at network automation and DevNet practices using Python, Ansible, and Terraform to improve reliability, security posture, and operational efficiency. Recognized for leading complex migrations, upgrades, and security transformations while ensuring business continuity and risk reduction.

TECHNICAL SKILLS

Firewalls & Secure Access	Palo Alto Networks (PA-7000, PA-5000, PA-3000, PA-1000 series, Panorama, GlobalProtect), Fortinet (FortiGate 60E, 200E, 500E, 1000, 1000F, 3200F, FortiManager, FortiAnalyzer), Cisco Firepower (4115, 4125, 4145), Cisco ASA 5506-X, 5508-X, Check Point (NGX, R65–R80, R77.30, R80.x), Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), Cisco Umbrella (DNS Security, SWG)
Data Center & Core Networking	Cisco Nexus (9300, 7000, 5000 series), Cisco Catalyst (6500, 4900, 4500, 3750, 3500, 2900, 6807), Cisco Routers (ASR9K, 7200, 3900, 3600, 2800, 2600, 2500, 1800), Arista (7050SX3, 7150S, 7160, 7260QX, 7508R, DCS-7280SR/QR), Juniper EX (2200, 2500, 3200), Spine-leaf architectures, EVPN/VXLAN, High Availability, Redundancy Design
Cloud & Hybrid Networking / Security	AWS (EC2, VPC, IAM, S3, CloudTrail, GuardDuty, Route53, CloudWatch, CloudFormation, ALB, Auto Scaling, Lambda, Athena, SNS/SQS, EMR), AWS Transit Gateway, AWS Direct Connect, AWS VPN, VPC Peering, AWS BGP Peering, Amazon Private Network Interfaces (PNI), Azure (NSGs, Azure Firewall, ExpressRoute, Azure MFA, Azure Log Analytics), GCP fundamentals, Hybrid and Multi-Cloud Security Architecture.
SOC Platforms & Blue Team Tooling	Splunk Enterprise, Microsoft Sentinel, ELK Stack, Microsoft Defender XDR, Defender for Endpoint, CrowdStrike Falcon, Carbon Black EDR, Tanium, Alert triage, log correlation, threat hunting, phishing and malware analysis, MITRE ATT&CK mapping, SOAR workflows, incident escalation and response
SOC Governance, Maturity & Compliance	SOC Auditing and Maturity Assessments (NIST CSF, ISO 27001, CISA SOC Maturity Model), KPI/KRI definition, executive reporting, audit readiness, Playbook and runbook governance, tabletop exercises, incident simulations, Analyst activity monitoring, least-privilege enforcement, RBAC, access reviews
Detection Engineering & Threat Analysis	SIEM use-case development, detection engineering, alert tuning, false-positive reduction, Threat intelligence integration, packet and PCAP analysis, Advanced malware sandboxing (VMRay), behavioral analytics
Query, Log & Data Analysis	Kusto Query Language (KQL – Advanced): Microsoft Sentinel, Azure Log Analytics, Defender XDR, hunting notebooks SQL (Proficient): complex joins, window functions,

	threat-hunting queries, Log parsing and enrichment using Splunk, ELK, PostgreSQL, MySQL
Penetration Testing & Vulnerability Management	Nmap, Nessus, Burp Suite, Gobuster, Hydra, Metasploit, John the Ripper, Hashcat, Web application and API penetration testing, CMS exploitation, credential attacks, privilege escalation, Container and DevSecOps security: Trivy, Clair, secure SDLC and CI/CD reviews
SD-WAN & Remote Access	Cisco Viptela (vEdge, vManage, vSmart, vBond), Prisma SD-WAN, Aruba S2500, 3800, Meraki MR30H, IPsec VPNs, VPN concentrators, AnyConnect posture assessment, Zero Trust Network Access (ZTNA)
Load Balancing & Application Delivery	F5 BIG-IP (i5000, r4000, r2000 – LTM, GTM, APM), F5 iRules, SSL Offloading, Citrix NetScaler, Cisco ACE 4710, AWS Elastic Load Balancer (ELB / ALB), Global Server Load Balancing (GSLB)
Network Monitoring & Troubleshooting	SolarWinds, Nagios, Cisco DCNM, FireMon, Wireshark, HP NNMi 8xi, NetFlow, Cisco Prime, tcpdump, Ethereal, Postman (API testing), NetBrain, latency and packet-loss analysis
Networking Protocols	RIP, OSPF, EIGRP, BGP, MPLS, STP/RSTP, VLANs, VTP, PAGP, LACP, HSRP, VRRP, GLBP, TACACS+, RADIUS, AAA, IPv4, IPv6, EVPN, VXLAN, VRF, Route leaking, RSVP, LDP
LAN & Wireless Technologies	Ethernet, Fast/Gigabit/10-Gig Ethernet, Port-Channel, 802.1Q, Cisco ISE NAC, Aruba ClearPass NAC, Aruba Air Monitors, Wireless Mesh Networking, RF interference analysis, secure WLAN design
Automation, Scripting & DevSecOps	Python (Pandas, NumPy), Ansible, Terraform, PyATS, CI/CD pipelines, Git, Jenkins, AWS SDK (Boto3), Shell scripting, API automation, firewall rule orchestration, infrastructure-as-code, Docker security
Frameworks, Standards & ITSM	NIST CSF, NIST 800-61 (Incident Response), ISO 27001, MITRE ATT&CK, OWASP Top 10, Zero Trust Architecture, ITIL Incident and Change Management, ServiceNow workflows and operational governance
Professional & Advisory Skills	Critical thinking, executive communication, technical documentation, client advisory engagement, security reporting, cross-functional collaboration, adaptability to emerging threats

PROFESSIONAL EXPERIENCE

Pledge Environmental | New Jersey, USA *July 2023 - Present*
Sr. Network Security Engineer

Responsibilities:

- Design, implement, and operate enterprise, data center, and hybrid-cloud network security architectures, supporting large-scale production environments with high availability, segmentation, resilience, and compliance alignment.
- Engineer and manage next-generation firewall platforms including Palo Alto (PA-7000/5000/3000/1000), Fortinet (FortiGate 60–3200F), Cisco ASA/Firepower, and Check Point, implementing User-ID/App-ID/Content-ID, URL filtering, NAT/PAT, SSL inspection, IPS, and site-to-site VPNs.
- Centralize firewall policy orchestration, logging, and lifecycle management using Panorama, FortiManager/FortiAnalyzer, Firepower Management Center, and Check Point SmartConsole, leading upgrades, migrations, and configuration standardization across environments.
- Design and deploy Zero Trust Network Access (ZTNA) and Secure Web Gateway (SWG) solutions using Zscaler ZIA/ZPA, Palo Alto GlobalProtect, Cisco Umbrella, and Bluecoat Proxy, integrating identity-aware controls with Azure AD and MFA.
- Architect and secure hybrid cloud connectivity across AWS, Azure, and GCP, including Transit Gateway, Direct Connect, ExpressRoute, VPN tunnels, VPC peering, PNIs, and BGP routing between cloud and on-prem data centers.

- Lead data center network design and modernization, deploying 100G spine-leaf architectures (eBGP), EVPN/VXLAN, Cisco ACI, and Arista CloudVision (CVP/CVX) to support consolidation, scale, and high-throughput workloads.
- Configure, troubleshoot, and optimize Layer 2/Layer 3 protocols including BGP, OSPF, EIGRP, MPLS, VRF, STP, LACP, VLANs, IPv4/IPv6, route leaking, and redundancy mechanisms across Cisco, Arista, Juniper, and Nexus platforms.
- Deploy and operate SD-WAN solutions across MPLS, DIA, and Internet VRFs using Cisco Viptela, Prisma SD-WAN, Meraki, and Aruba, enabling application-aware routing for voice, video, and business-critical traffic.
- Design and support enterprise LAN and wireless infrastructures, deploying Cisco Catalyst, Aruba switching, Cisco WLC, Aruba Mobility Controllers, Mist/Juniper WLAN, and wireless mesh solutions, including RF surveys (Ekahau, AirMagnet) and high-density WLAN optimization.
- Implement Network Access Control (NAC) and segmentation using Cisco ISE and Aruba ClearPass, delivering 802.1X wired/wireless authentication, posture assessment, SGT-based segmentation, and device classification across diverse endpoint populations.
- Integrate Layer 4–7 services including F5 BIG-IP (LTM/GTM/APM), Citrix NetScaler, Cisco ACE, and application delivery controllers with Cisco ACI and traditional networks to optimize traffic flow, availability, and application performance.
- Operate and monitor enterprise infrastructure using SolarWinds, FireMon, Infoblox, NetFlow, SNMP, Wireshark, Splunk, and related platforms; administer DNS, DHCP, and IPAM services in highly available grid environments.
- Monitor, triage, and investigate security alerts from SIEM platforms (Microsoft Sentinel, Splunk, Elastic, QRadar), EDR/XDR tools (CrowdStrike Falcon, Microsoft Defender, Carbon Black, SentinelOne), and cloud-native detections (AWS GuardDuty, Azure Defender for Cloud).
- Perform initial containment actions, including endpoint isolation, IP/hash blocking, account disabling, and malicious domain sinkholing.
- Conduct in-depth incident analysis using log correlation, packet captures (PCAP), memory artifacts, and malware sandboxing (VMRay, ANY.RUN, Hybrid Analysis, URLScan).
- Perform proactive threat hunting using advanced KQL, Splunk SPL, Sigma, and YARA rules, identifying stealthy or emerging threats across network, endpoint, and cloud telemetry.
- Document incidents in case management and ticketing systems (ServiceNow, Jira, TheHive), providing clear timelines, indicators of compromise, and MITRE ATT&CK mappings, and escalate confirmed incidents to L3/IR teams and leadership with actionable handover notes.
- Tune and optimize detection rules and correlation logic to reduce false positives, improve signal-to-noise ratio, and enhance detection fidelity.
- Author, maintain, and validate incident response playbooks and runbooks for scenarios including phishing, ransomware, lateral movement, data exfiltration, and BEC, and participate in purple-team and tabletop exercises.
- Generate daily/weekly SOC shift reports and contribute to monthly KPI/KRI reporting (MTTD, MTTR, detection coverage, false-positive rate) for executive and audit audiences.
- Enrich alerts with threat intelligence from internal sources and platforms such as MISP, OTX, VirusTotal, and Recorded Future.
- Support vulnerability management efforts by correlating scan results (Nessus, Qualys, Defender Vulnerability Management) with active exploitation indicators and detection telemetry.
- Assist with forensic evidence collection and chain-of-custody preservation during major incidents and regulatory investigations
- Develop and maintain network and security automation using Python, Ansible, Terraform, PyATS, and CI/CD pipelines (Git, Jenkins) to automate configuration management, testing, inventory collection, and reporting.
- Support DevSecOps and cloud automation, building Python-based workflows for AWS auto-scaling, CloudWatch monitoring, API testing (Postman), and Lambda functions, with unit and integration testing using pytest.

- Produce and maintain security and network documentation, including architecture diagrams, policies, configurations, incident reports, audit artifacts, and operational runbooks, ensuring readiness for compliance and regulatory reviews.

SOFTCOM Solutions SA (Pty) Ltd *Mar 2018 – Oct 2018*
Infrastructure and Software Application Support Engineer (Tier-2/3)

Responsibilities:
- Provided Tier-2/3 infrastructure and application support for enterprise environments, supporting both production and non-production systems across on-prem and hybrid cloud platforms.
- Supported Azure hybrid infrastructure, including cloud-to-on-prem integrations, virtual machines, backups, and recovery operations; performed server installations, upgrades, and maintenance for Windows and Linux systems.
- Troubleshot and resolved complex network and security issues involving TCP/IP, DNS, DHCP, VLANs, routing, firewall rules, access controls, and inter-VLAN routing, ensuring minimal service disruption.
- Deployed and managed Cisco ASA firewalls at branch and data center locations, configuring static routes, NAT, and IPsec site-to-site VPN tunnels to securely connect remote sites and client networks.
- Implemented and supported remote access solutions including IPsec VPN, SSL VPN, Easy VPN, Citrix Access Gateway, and Citrix Secure Gateway, collaborating directly with clients to streamline onboarding and secure connectivity.
- Engineered and optimized application delivery and load balancing using F5 LTM and Citrix NetScaler ADC, configuring VIPs, pools, SSL offloading, content switching, HA clustering, and performing firmware upgrades and health checks.
- Migrated load-balancing infrastructure from virtual to physical F5 appliances, resolving performance and memory-leak issues while improving application stability and throughput.
- Designed, configured, and administered network monitoring solutions using PRTG, SolarWinds, SNMP, and custom sensors, enabling proactive alerting, performance visibility, and rapid incident response.
- Integrated monitoring platforms with Datadog and automated alert workflows to reduce downtime and accelerate fault isolation.
- Developed Ansible playbooks and roles to automate multi-vendor network configurations (Cisco Routing & Switching, Nexus, ACI), enabling consistent, repeatable, and audit-compliant changes across environments.
- Built Python automation scripts (using Paramiko) to streamline firewall ACL updates and IP whitelisting on Cisco ASA devices, significantly reducing manual configuration effort.
- Supported FortiGate firewall policy design and enforcement, collaborating with third-party vendors on IP migration strategies and security posture improvements.
- Managed data center infrastructure and circuits hosted in Flexential facilities (Chaska and Aurora/Denver), supporting redundancy, production-backup synchronization, and operational continuity.
- Configured and maintained pfSense and DrayTek firewalls for content control, traffic optimization, and perimeter security in customer environments.
- Led the migration of Active Directory environments from Windows Server 2012 to 2016, coordinating backups, validation, and post-migration support.
- Created and maintained technical documentation, including SOPs, incident reports, change records, Visio rack diagrams, and network topology diagrams to support operations and audits.
- Provided client-facing production support, resolving VPN and connectivity issues with a 95% resolution rate, and delivered transition and handover documentation during resource attrition scenarios.
- Collaborated closely with internal teams, customers, and developers to gather technical requirements, deliver off-site software application support, and ensure seamless handoffs during high-priority incidents.

DPoint Information Technologies *Feb 2012 – Nov 2016*
Systems and Network Engineer

Responsibilities:

- Designed, implemented, and supported enterprise LAN/WAN infrastructures across multi-site environments, providing Layer 2 and Layer 3 network engineering from initial design through production deployment and operational support.
- Delivered end-to-end routing, switching, and WAN services, configuring VLANs, IP addressing, inter-VLAN routing, trunking (802.1Q), STP/PVST, HSRP, and dynamic routing protocols including OSPF, policy-based routing, and link-state routing across Cisco enterprise platforms.
- Installed, configured, and maintained Cisco routers and switches including 7200/3800/3600/2800/2600/1800 routers, Catalyst 6500/4500/3750/3550/2900, and Nexus 2K/5K/7K/9K, supporting campus, data center, and WAN connectivity.
- Led network build-outs for new locations, managing migrations, hardware refreshes, and scheduled maintenance while supporting MSP/NOC operations, escalations, and root-cause analysis (RCA).
- Engineered and operated enterprise firewall and perimeter security solutions, deploying and managing Palo Alto Networks (PA-7000/5400/5450), FortiGate (1000F/2600F/4800F), Cisco ASA/Firepower (FTD), and Check Point firewalls, including policy design, NAT, VPNs, IPS, application control, and web filtering.
- Implemented User-ID, GlobalProtect, IPSec site-to-site VPNs, remote-access VPNs, and secure access controls across enterprise and branch environments; led firewall migrations including Check Point FW-1 to Cisco ASA and ASA upgrades from 8.x to 9.x with Firepower services.
- Centralized security and firewall management using FortiManager, Firepower Management Console, and vendor-specific platforms; monitored firewall activity and security events using logging and reporting tools.
- Designed and managed application delivery and load-balancing platforms, including F5 BIG-IP (LTM, GTM, APM, ASM), Citrix NetScaler, Cisco ACE, and A10 GSLB, implementing VIPs, pools, iRules, SSL offloading, health monitoring, and global server load balancing across data centers.
- Performed NetScaler-to-F5 migrations, collaborated with application and DNS teams, and produced detailed engineering documentation for LTM/GTM change and release processes.
- Leveraged F5 TMOS/TMSH for advanced configuration, HA synchronization, diagnostics (tcpdump, dig, ping), hotfix installation, qkView generation, and vendor troubleshooting with F5 support.
- Implemented and supported SD-WAN solutions using Cisco Viptela, including IPsec encryption, secure overlay design, and integration with enterprise routing and authentication policies.
- Designed and supported enterprise wireless networks, deploying Cisco Meraki and Cisco/Aruba WLAN solutions, optimizing RF performance, roaming, and security in high-density environments; led migrations from legacy wireless to Meraki-based mesh architectures.
- Implemented 802.1X wired and wireless authentication using Cisco ISE, ACS, and RADIUS/TACACS+, delivering role-based access, SGT segmentation, posture checks, and device classification across diverse endpoint types.
- Led NAC initiatives using Cisco ISE 2.x, integrating Active Directory, RSA SecureID, PEAP, and EAP-TLS authentication, downloadable ACLs, and scalable group tags (SGT) across enterprise switches.
- Configured and maintained DNS, DHCP, and IPAM services, including Infoblox appliances, managing DHCP scopes, enterprise IP addressing, and network service availability.
- Deployed and operated network monitoring and performance platforms including SolarWinds NPM, Wireshark, NetBrain, SNMP, NetFlow, and NDC Flex Flow, enabling proactive fault detection, capacity planning, and MTTR reduction.
- Developed network automation and scripting solutions using Python and Ansible, automating firewall rule deployment, switch configurations, log collection, reporting, and operational workflows to reduce manual effort and incident response times.
- Supported SDN and data center technologies, including Cisco ACI, VDC/VPC configurations on Nexus 7K/5K, FabricPath, ISSU upgrades, and integration of Layer 4–7 services.
- Designed and documented network architectures using Microsoft Visio, supporting server, application, and data center deployments across multiple locations.

- Participated in cloud and hybrid initiatives, supporting early AWS deployments, Auto Scaling architectures, and serverless components (Lambda, API Gateway) for application migration and availability improvements.
- Implemented and supported secure web, email, and threat protection platforms, including McAfee Web Gateway, Bluecoat Proxy, Cisco Umbrella, IronPort, FireEye (NX, EX, HX, Helix), and Stealthwatch for anomaly detection.
- Performed advanced troubleshooting for complex data center, LAN, WAN, wireless, and security incidents, collaborating with cross-functional teams to restore service and improve long-term stability.

Verde Information Technologies *Jan 2011 – Jan 2012*
Database, Systems and Network

Responsibilities:
- Administered and supported enterprise on-premises databases (MySQL and Microsoft SQL Server) hosted on Windows Server platforms, performing installation, configuration, user management, backup/restore, patching, and basic performance tuning for business-critical applications.
- Coordinated database schema updates, access control changes, and data growth planning in collaboration with application developers, ensuring database availability, data integrity, and security compliance.
- Monitored database performance, storage utilization, and query execution behavior, identifying bottlenecks related to indexing, disk I/O, and memory allocation, and implemented corrective actions to improve reliability and scalability.
- Designed and maintained structured data repositories and reporting databases used for operational and management reporting, supporting early data warehousing-style workloads including historical data retention, aggregation, and scheduled data refresh processes.
- Assisted in data modeling activities, defining basic relational schemas, table relationships, and data standards to support reporting, backup consistency, and long-term maintainability.
- Implemented database security controls, including role-based access, firewall rules, network segmentation, and backup encryption to safeguard sensitive organizational data.
- Installed, configured, and maintained Windows Server (2000/2003) systems supporting Active Directory, DNS, DHCP, Exchange Server, FTP services, and database platforms, ensuring high availability and system integrity.
- Performed system monitoring and log review for servers, applications, and databases; verified completion of scheduled jobs including database backups, maintenance tasks, and batch processes.
- Implemented and tested automated backup and recovery strategies for servers and databases, regularly validating restore procedures to meet business continuity and disaster recovery requirements.
- Designed, implemented, and supported enterprise LAN/WAN infrastructure, configuring Cisco routers and switches (Cisco 3745, 1800/3900 series routers; Catalyst 6509/3560/2960 switches) across multi-site environments.
- Delivered Layer 2 and Layer 3 networking, configuring VLANs, inter-VLAN routing, trunking (ISL/802.1Q), STP/RSTP, EtherChannel, NAT, SNMP, and routing protocols including RIP, OSPF, EIGRP, BGP, static and policy-based routing.
- Supported site-to-site WAN deployments, VPN connectivity, and multi-location troubleshooting, coordinating infrastructure changes with systems and security teams.
- Administered network and database access controls, managing internal and external user accounts, permissions, and security settings across servers, databases, and network devices.
- Engineered perimeter security solutions, configuring Cisco PIX and ASA firewalls (5540/5550/5585), implementing DMZ architectures, NAT policies, IPsec/GRE tunneling, and firewall rule tuning.
- Supported load balancing and traffic distribution between core and access layers using F5 network load balancers, improving application availability and database access reliability.

- Conducted systems and network analysis to evaluate existing infrastructure, identify performance gaps, and recommend improvements to hardware utilization, database storage allocation, network segmentation, and system workflows.
- Worked closely with business users, developers, and management to analyze application requirements, data processing needs, and system limitations, translating them into technical solutions and implementation plans.
- Produced technical documentation covering system architecture, database configurations, data flows, network topology, backup procedures, and operational workflows.

PROJECTS

Network Security Monitoring & Intrusion Detection System | *GitHub*

- Implemented Python-based traffic monitoring to detect anomalous network behavior
- Improved visibility into network activity and reduced false positives

Web-Based Network Intrusion Detection Platform | *GitHub*

- Built real-time traffic visualization to support security incident investigation.
- Enabled detection and visualization of suspicious traffic patterns to support security operations and incident response.

CERTIFICATIONS

- Cisco Certified Network Associate (CCNA)
- Oracle Database 10g Administrator Certified Associate (OCA)
- Oracle Database 10g Administrator Certified Professional (OCP)
- Cybersecurity Certificate

EDUCATION

Doctor of Philosophy (PhD) in Electronic Engineering	Stellenbosch University, Stellenbosch, South Africa	Apr 2020
Master of Science (MSc) in Electrical Engineering	University of the Witwatersrand, Johannesburg, South Africa	Mar 2017
Bachelor of Science (B.Sc.) in Mathematics	University of Ibadan, Ibadan, Nigeria	Nov 2009