IT PROFESSIONAL

Highly accomplished Information Technology professional with 10+ years of experience and extensive expertise as an Enterprise Network Engineer, Network Security Engineer and Cloud Network Engineer. Skilled at working in fast paced, team-oriented environments, while providing staff with technical solutions to facilitate demanding requirements. Adept at collectively collaborating with report writers, architects, developers, desktop support and systems support personnel. Recognized among leadership as being a highly motivated, and self-starter who is willing to take on new challenges and contribute to being a great team player.

CORE COMPETENCIES

Analytical | Adaptability | Technical Acumen | Business Operations | Tenacity

CERTIFICATIONS | PROFESSIONAL TRAINING

- Palo Alto Certified Network Security Engineer (PCNSE): Verification #: 876D7ETKD1B4139W
- AWS Advanced Network Specialty - Certified (Validation Number 96a1a80675b64068abd4338b405b31a7)
- Fortigate Firewall: NSE 4 Network Security Professional - Validation Number IkmVf37Qqk
- CISCO INTERNETWORKING: CCNA, CCNP Enterprise (Validation Number: Y5RLPDDFJKFQQBCL)
- Azure Networking Specialty - Certification Number: I484-4431
- GCP Certified.

TECHNICAL SKILLS AND TECHNOLOGY STACK

Enterprise Networking and Cyber/Network Security: Installation and configuration of Catalyst Series Switches using IOS XE (9606, 9500, 9300 Stacked switch). Routing Protocols (EIGRP, OSPF, BGP, Static Route and Default Route), MPLS Connection, Silver Peak SD-WAN, IPsec VPN (Site to Site and Client Remote connect), NAT, Access-list, DNS, DHCP, Port Security, Port Channels, Vlans, STP, VTP, SVI, Trunk/Access port, High Availability, Data center Cable Management (Copper, Fiber Distribution and troubleshooting). Analysis of network traffic and monitoring Network using Opsview, Wireless Controller and Wireless Analyzer. Installation, configuration and management of Palo Alto Firewalls, Panorama, Prisma Access SASE, Splunk administration/logging, FortiGate Firewall configuration/Administration.

Cloud Network and Security:

- Monitoring & Event Mgt: AWS CloudWatch, AWS S3, Cloud Trail, VPC flow log logging Policy/Cross Account logging.
- Identity & Access Mgt: AWS Organization, AWS IAM, Active Directory.
- AWS Governance & Compliance/ Architecture and Networking: AWS Organization, Landing Zone/ AWS Control Tower, VPC/vpc peering, vpn gw, trasit-gw, direct connect gw, ELB, CloudFront, VPN AWS Network Manager, Resource Access Manager, AWS endpoint, endpoint private link etc.
- Data Protection/ Self Service: AWS Certificate Manager, AWS KMS, SG, AWS Cloud HSM, S3 policies and SSS-KMS.
- Azure Cloud: Azure architecture, management group, subscriptions, resource group, vnet/subnets, virtual machine, virtual machine scale set, Azure availability-set, Azure AD, DNS zones, User-defined route, virtual network gateways, Application security groups, Azure Firewall, Azure Express-route, Azure Load Balancer, Azure Application gateway, Azure Web Apps, Azure traffic Manager, Azure Front Door, Azure Virtual Network NAT, Azure Point to Site VPN, Azure Site to site VPN, Azure Virtual WAN-Hub, Azure Endpoints and Implement Private access to Azure services, etc.
- Application Delivery/Orchestration/Automation/IAC: Jenkins, AWS CI/CD pipeline, Terraform, Python and Ansible.

EXPERIENCE

Mid-Sized MSP **December 2021 - Present**

Sr Cloud Network Engineer/Network Security Engineer

Provides day-to-day steady support services for all core network technologies, Cloud Network services and security services.

- Resolve ticket from customers, assist tier 1&2 engineers with complex issues, work with vendor supports to resolve complex issues, and project implementation.
- Design, implement, and maintain secure cloud network architectures across multiple cloud platforms (e.g., AWS, Azure, GCP), such as deploying Security vpc with Palo alto HA, etc.
- Design, configure and manage next-generation firewalls such as, Palo Alto, fortigate, Cisco Firepower, AWS firewall. Cloud security with security-group, nsg to enforce security policies and protect cloud/on-prem infrastructure.
- Design, configure and manage enterprise network devices such cisco routers, cisco/aruba switches and wireless radio/devices.
- Switch configurations such as vlans, svi, switchport access, switchport trunk, allow vlans trunk, port-channel, STP, etc.
- Enterprise core network/cloud routing such as Eigrp, Static route, ospf, bgp, firewall vpn site-to-site, cloud/on-premise site-site, cloud to cloud vpn site-to-site, global-protect, aws client, azure client, Transit-gw, Direct-connect gateway.
- Design, implement and manage network availability and optimize performance using load balancers, cloud multi-zones, HA/Failover connectivity and QOS.
- Network and traffic monitoring for potential threats, anomalies and troubleshooting via Firewall traffic logs, threat logs, flow log, CloudWatch logs, Cloud trail logs and etc.
- Develop and enforce cyber/network security policies, procedures, regulatory compliance with industry standards such as PCI, PHI, GDPR, HIPAA.
- Excellent troubleshooting skill for enterprise complex network environment, Palo Alto firewall, other firewalls/security issues in the cloud and on-premise environments.
- Design, implement and manage Strata Cloud Manager, Panorama, Palo alto firewall and configurations such as HA, Network objects, NAT Rule Policy, Malware/file policy, SSL Policy, Prefilter Policy, APP-ID, USER-ID, URL Filtering, Network Analysis, APP-ID, USER-ID, URL Filtering, Global Protect, Virtual Route, Security Profiles, IPsec VPN Site to Site, zero trust architecture, Prisma Access SASE and Client Remote connect VPN.
- Automating network Infrastructures using infrastructure-as-code tools such as Terraform, Python, and Ansible.
- Identified, analyzed and resolved infrastructure vulnerabilities and application deployment issue. Collaborate with infosec team to conduct regular security assessments and penetration testing to identify vulnerabilities.
- Collaborate with cross-functional teams to ensure network security aligns with business objectives.
- Stay current with emerging cloud technologies and security threats to maintain a robust security posture.
- Develop and update network diagrams, IP address scheme and documentation of troubleshooting steps as well as implementation step, monthly Backup for Disaster network devices config, Network and security check-list and device OS upgrade.

Manufacturing Firm **March 2020 - December 2021**

Network Engineer

Implemented and maintained Routers and switches, Palo Alto firewall/Panorama, Cisco firepower/FMC, Fortigate Firewall, other firewalls both on the cloud and on-premise. Configured/deployed firewall server profile/mfa. Designed, deployed and managed Cloud security resource such as AWS firewall, security hub, security-group, AWS firewall, AWS config, Azure firewall and azure nsg, etc.

- Enterprise Switching such as vlan configuration, svi, switchport access, switchport trunk, allow vlan trunk, port-channel, STP. Enterprise Routing such as Eigrp, Static route, ospf, bgp, cloud and on-premise wireless controller and APs etc.
- Deploying Managing on-premise Enterprise Network Security. Implementing High Availability, Network objects, Access Control Policy, NAT Rule Intrusion Policy, Malware/file policy, SSL Policy, Prefilter Policy, APP-ID, USER-ID, URL Filtering, Network Analysis, APP-ID, USER-ID, URL Filtering Global Protect, Virtual Route, Security Profiles, IPsec VPN Site to Site and Client Remote connect VPN, maintenance of Palo Alto firewall as such software upgrade and licensing.
- Design, deploy and manage AWS network resources such as vpc, subnets, aws instances, route tables, internet-gw, natgw, transit-gw, vpn-gw, route53, direct-connect, aws shield, wap, load-balance, CI/CD Pipelines, Jekins, Terraform IAC.
- Design, deploy Azure network such as resource group, vnet/subnets, virtual machine, Azure AD, azure availability set/scale set, user-defined route, virtual network gateways, nsg, express route, azure application gateway, azure traffic manager, azure front door, azure web app, azure virtual network nat, azure network watcher, azure endpoint services, etc. Design and deploy Disaster Recovery environment on AWS/Azure cloud and deploy Hybrid cloud.
- Troubleshoot tickets from Auto-task, assist desktop support engineers, work with vendor supports to resolve complex issues and project meeting/implementation.
- Develop and update network diagrams.

Construction Firm **March 2017 – March 2020**
Network Engineer

- Installation, setup and maintenance of New LAN/WAN Network Infrastructures such as Layer 3 Catalyst Switches (9606, 9500, Stacked 9300), Nexus 9k switches, Silver Peak SD-WAN, Cisco firepower Firewall with FMC and Palo Alto Firewall with Panorama, Cisco Wireless Controller, wireless APs, Aruba Wireless Radio on AGV carts for production, APC UPS batteries, Monitoring of Network Infrastructures mentioned above via Opsview Cloud, and Develop and update network diagrams, IP address scheme, documentation Backup of Network Devices, Daily Check-list/Network Infrastructure Health Checks.
- Managed provisioning of AWS infrastructures using Terraform and AWS console.

ADDITIONAL RELEVANT EXPERIENCE

Network Engineer, Oil & Gas Firm - June 2013– Dec 2016
Network FIELD Engineer, Communications Firm - Feb 2007- Apr 2013

EDUCATION

Bachelor of Science, (B.Sc) Banking and Finance (1999–2005)
University of Calabar, Calabar, Cross State, Nigeria