**Chinyelugo augustine Umenwaliri**

chinyelugoumenwaliri@aol.com |(757) 303-3109

**Summary**

IT professional with over 24 years of professional and progressive experience in implementation, configuration, escalation support/ticket resolution and troubleshooting of various technologies which includes proficiency in security, firewalls, routing, routing protocols, switching technologies;- **Cisco Routers ASRs/ISRs, Cisco Catalyst/Nexus (3,5,7,9K)Cisco ASA firewalls, Palo Alto, Checkpoint Firewall, Juniper SRX series, F5 Big IP, AAA - TACACS+/RADIUS, SSH, VPN, SSL/IPSec, Port Security, RIP, OSPF, EIGRP, BGP, MPLS**,  **Wireshark, Cacti, Nagios, ForeScout and Solarwinds** .

**Experience/Accomplishments Highlights**

* Proven background and experience in reviewing design documents and implementing/deploying technologies including provisioning, deploying, configuration, validation, and documentation in a timely and proficient manner based on following internal policies and procedures and mandated compliances.
* Strong proficiency with administration and support including handling change requests, Tier 2 and 3 escalated tickets based on service level agreements (SLA) and documentation administration.
* Work well independently and in a team, environment including verbal and written communications with technical and non-technical professionals, third party vendors/service providers and clients.
* Proven skills as subject matter expert (SME) to both technical and non-technical professionals including acting as advisor/mentor for various technical, professional, and operational activities.

**Technical Certifications & Skills**

* Security Firewall Administrator **SFA**
* Cisco Certified Network Associate – Routing & Switching **CCNA**
* Cisco Certified Network Professional **CCNP**
* Juniper Network Certified Network Associate, Junos **JNCIA-Junos**
* Juniper Network Certified Associate, Security **JNCIA-SEC**
* PaloAlto Network Certified Network Security Engineer **PCNSE**
* Microsoft Azure Architect Technologies **AZ-300**

**Technical Skills Detail**

**Routing/Switching Technologies -** Cisco Routers ASRs/ISRs, Cisco Catalyst/Nexus, Juniper, Citrix, and H3C Routers & Switches, WAN, LAN, TCP/IP, Cisco IOS, Spanning Tree Protocol, BPDU, CDP, ACL, NAT, PAT, RIP, OSPF, EIGRP, BGP, MPLS, VTP, SNMP, SMTP, Static & Stub Routing, VLAN Trunking, Multicast, HSRP, SVI, CEF, VSS, VPCs.

**Security/Firewalls Technologies -** Cisco ASA firewalls, Cisco Security Manager Suite, Cisco IPS/IDS, Cisco ISE, Checkpoint Firewall, Juniper SRX series, Palo Alto, AAA - TACACS+/RADIUS, SSH, VPN, SSL/IPSec, Port Security

**Monitoring/Data Center Technologies/APPS** **-** Wireshark, Cacti, Nagios, Solarwinds, Sniffer, Orion, Remedy – VMWare, F5, Citrix Netscaler, Cisco AnyConnect, Cisco Prime, Meraki, SNMP, DNS, DHCP, FTP, Telnet, HTTP(S), SMTP, SFTP

**Voice Technologies –** VoIP/SIP, CUCM, UCCM, UCCX, RSTP, STP, Quality of Service (QoS), PoE, MMDS, LMDS, CVP, IVR, PBX/PBS. GSM, Cisco, Siemens, Alcatel, PBX, Huewai, PSTN,

**Wireless Technologies -** Cisco WLC, IEEE 802.1x & 802.11, WLAN, WAP, AP, LWAPP, Aironet,

**Other Technologies/Languages** – VMware, Active Directory, Exchange 2003/2007/2010, SQL Server, Windows NT, 2000, 2008, 2012, MAC OS, MS Office, 2003/2007/2010

**Summary of Professional Experience**

**WIPRO|Comcast (New Jersey) Sr. Network Security Engineer 2019–Present**

**INFOSYS|CenturyLink (Colorado) Network Security Engineer 2018–2019**

**Careernation (Arizona Mentors) Network Engineer (NSA) 2015–2017**

**Siemens ICN Sr. Network Engineer (TSE) 2002–2014**

**Education**

**Bachelor of Science in Computer Science & Engineering Enugu State University of Science and Tech**

**Master of Science in Information Technology, Security Management Colorado Technical University**

**Professional Experience Detail**

**Infosys| AAA Sr. Network Security Engineer March 2021–Present**

**Palo-Alto (Migration) and Fortinet Responsibilities**

* Configure, Manage and Monitor **Palo Alto firewall** models (Specifically the **PA-5050** and the **PA-5260**).
* Performed migrations from of **25Nos** **Check Point and 23Nos Cisco ASA firewalls** to **Palo Alto** using the **PAN Migration Tool MT3.3**
* Implement advanced Palo Alto Firewall features like **URL filtering**, **User-ID**, **App-ID**, **Content-ID** on both inbound and outbound traffic.
* Enable file forwarding to Wildfire cloud through Content-ID implementation to identify new threats.
* Leveraged Palo Alto Networks’ Wildfire inspection engine to prevent Zero-Day attacks.
* Manage multiple Palo Alto firewalls centrally through the Palo Alto Panorama M-500 centralized Management appliance.
* Implement the **Global Protect VPN, IPSec VPNs and SSL VPNs** through **IKE** and **PKI** on **Palo Alto** firewalls for site-to-site **VPN** Connectivity.
* Deployed Active/Standby modes of **High Availability (HA)** with Session and Configuration synchronization on multiple Palo Alto firewall pairs. Knowledge on the application of Active/Active HA mode.
* Enforce policy checks on north-south and east-west data center traffic through **Panorama M-500**. Provided escalated technical support in troubleshooting firewall and network issues.
* **Fortinet Firewall** administrator, configuration of **FortiGate 3000, 3815** series as per network diagram
* Managed firewall using **FortiGate** to allow or block IPs, created policies added different interfaces and VLANs installation, and implementation VPN
* **Fortinet Firewall** log review and analysis and troubleshoot connectivity issues
* Maintain current network posture with **Fortinet FortiGate** firewalls **300, 1000, 2000, and 3700** appliances

**Azure Responsibilities**

* Working as Cloud Administrator on Microsoft Azure, involved in configuring machines, storage accounts, resource group
* Remote login to Virtual Machines to troubleshoot, monitor and deploy application
* Configuration of Microsoft DevTest Labs to migrate the virtual machines from one subscription to another subscription
* Creating Labs, Virtual Machines along with setting up policies and using Formulars and Custom to deploy the network
* Managed Virtual Networks in Azure, established 13 core services in the VNET, and ensured Azure served in the MLP’s network

**WIPRO|Olympus Corporation Sr. Network Security Engineer June 2020–March 2021**

**Firewalls Responsibilities**

* Supports **Cisco Firepower** services and implementing and tuning IPS signatures.
* Provided technical and vendor support services, and planning Network Planning, Implementing, Configuring, **Juniper SRX210, SRX240**
* Configure and Install **Cisco NGFW Firepower** and **FTD** firewalls at multiple customers.
* Using the the Cisco Firewall Management Console (FMC) to utilize the API in the FMC to migrate ASA rules and objects to FMC
* Provide **DMZ/DDoS/VPN** Infrastructure Engineering and secured services to various LOB and B2B customers across various **DMZ Zones**. includes global DDoS detection and mitigation service, **DMZ,** B2B/extranets, encryption, Internet portal, and VPN while providing network level HLD and LLD designs. and solution delivery.
* **Viptela and Meraki SD-WAN** Deployment. Team lead for deployment, worked with the team to implement industry leading **SD-WAN infrastructure** to provide secure, carrier-independent WAN connectivity across enterprise.
* Configure **WAN connection with Meraki SD-WAN**
* Provide support for **DMZ’s** creating and developing DMZ designs IDS signatures to meet new and emerging technologies threats.
* Profound working knowledge of administration and management of **Palo Alto firewalls** using **Centralized Panorama M-100** and **M-500** devices
* Monitoring and troubleshooting traffic on **PaloAlto-5020 /2020 firewall**.
* Creating and modifying rules and objects on **PaloAlto-5020/2020 firewall**
* Configuring and deploying **Global Protect VPN** with multiple Gateway and rolled out to 30k+ users.
* Troubleshooting and implementing the **Palo Alto Global Protect VPN**
* Managed configuration, deployment, and operational support of **FIPs**, PED enable Hardware Security Modules (HSMs)
* Use **FIPS-compliant algorithms** for encryption, hashing, and signing*.*
* Analyze logs and make necessary network report using smart reporter console application.
* Configure **IPSEC** and **SSL VPN** with **Palo-alto**, **Cisco ASA**, **Fortinet**, **Checkpoint** and **Router**.
* Manage and configure the **Cisco ASA 5585** and **ASA 5525 Firewalls** to maintain network security and provide **IPSEC LAN** to **LAN VPN** to vendors and business partners. Utilize **AnyConnect** remote access **VPN** and certificate base VPN for all employees and vendors.
* Configure and install the Cisco IPS modules integrated in the **ASA5585** Firewall to monitor and block unwanted traffic as a security measure.
* Monitoring and alert management of all components related to the **Cisco ISE** solution
* Troubleshoot firewall issues using **CLI** and **GUI**.
* Manage **Palo alto**, **Checkpoint**, **Cisco ASA** and **Fortinet** policy and network.
* Creates, and maintains Bluecoat proxy policies.

**WIPRO|Comcast (New Jersey) Sr. Network Security Engineer June 2019–June 2020**

**Firewalls Responsibilities**

* Utilized **ForeScout** to create lists of devices imported from a third-party source to determine which authorized devices are disconnected from the network at any given time.
* Configured the monitoring solution in ForeScout, and executed a systematic gamut of checks, to ensure network monitoring accuracy.
* Provide **DMZ/DDoS/VPN** Infrastructure Engineering and secured services to various LOB and B2B customers across various **DMZ Zones**. includes global DDoS detection and mitigation service, **DMZ,** B2B/extranets, encryption, Internet portal, and VPN while providing network level HLD and LLD designs. and solution delivery.
* Provide support for **DMZ’s** creating and developing DMZ designs IDS signatures to meet new and emerging technologies threats.
* Back up, Restore and upgrade of **CheckPoint** and **Fortigate** firewall appliances.
* Fortigate **S2S & SSL VPN** Implementation
* Analyze logs and make necessary network report using smart reporter console application.
* Configure checkpoint and fortigate firewall to authenticate users based on user identity, user group, session and PC-User Authentication.
* Creates, and maintains Bluecoat proxy policies.
* Implementation of **Bluecoat proxy**, implementing authentication using client certificate and SSL interception using Client Sub CA certificates
* Troubleshooting issues of internet traffics via **Bluecoat Proxy.**
* Worked or **Bluecoat proxy SG500-20**, and CAS appliance implementation for client\’s Internet traffic

**Aruba Responsibilities**

* Routing and Switching experience with **EIGRP, OSPF and BGP configuration**, troubleshooting, configuration of **DHCP and DNS** on routers and switches at various remote site Designs
* Design and setup of **Aruba Controllers 7200 and 7400** series and stacking switches 3800 series
* PCI Compliance auditing with Cisco/Aruba Wireless Security Assessments and Wireless Site Surveys
* VPN implement and troubleshoot IP-SEC tunnels, GRE Tunnels, SSL-VPN on Aruba Controllers
* Aruba Switch **s3500 & 3810** Complex Stacking topologies and profile configurations
* **Aruba ClearPass** server Authentication: **802.1X, AAA**, Policy Management, Guest Access, **B.Y.O.D.**
* Perform standard configuration, management, and maintenance tasks for Linux servers, requests, escalation support/ticket resolution and analysis in an enterprise **LAN/WAN** environment for datacenters, corporate, WAN links, and branch offices.
* Technologies include but not limited to routing, switching, security, wireless and voice throughout an enterprise network of corporations from data center, corporate, **WAN** links to regional and branch offices.
* Other activities included as needed and schedule reports to senior management on the status of technical implementation activities, professional/technical review on **LAN/WAN** Professionals and its overall success, monitored and worked to streamline/improve the company’s standards and processes.

**F5 Big IP Responsibilities**

* Collaborating with Application owners, Network Team, DNS Team, and Firewall Team, to migrate applications from Legacy Juniper Pulse Secure Load Balancer to New **F5 BIG-IP** Local Traffic Manager
* Migration of applications from **Juniper Pulse Secure** to **F5 LTM**.
* Maintenance and analysis of the **F5** network for any possible up-gradation
* Configured and troubleshooting the **F5 LTM** and providing level 2 support for the customers.
* Created the **AAA** servers for **LDAP** and **AD** authentication in **F5 APM**.
* Implemented SSO with **F5 Application Policy Manger** and Active Directory for various applications
* Designed and maintained **F5 APM SSO** and two factor authentications for remote virtual desktop infrastructure.
* Worked on BIG-IP Access Policy Manager (APM) contextually secures, simplifies, and protects user access to apps and data
* Implemented Web traffic load balancing function and manipulated.
* Configured **SSL** offloading, bridging and pass through for custom applications per business needs.
* Handling various trouble tickets, firewall rule changes, assisting other teams to bring the device to production, making **DNS** changes and routing changes.
* Extensive knowledge of Load balancing technology including algorithms and health check options
* Extensive knowledge and experience with hosting **SSL** certificates on the **F5 BIG-IP** platform
* Extensive knowledge and experience regarding **F5 BIG-IP LTM VIP** configuration with health check
* Extensive knowledge and experience with **F5 BIG-IP GTM** Wide IP configuration
* Knowledge and experience with **F5 BIG-IP** iRule programming and troubleshooting experience

**Citrix Netscaler Responsibilities**.

* Handling of Citrix Farm & Zone creation, Citrix Servers installation, server configuration and managing
* Performing Pre-installation tests and Post-installation tests for Citrix components and applications on test servers.
* Installing, configuring and administering all the Windows Infrastructure & Application servers.
* Monitor, optimize and troubleshoot Citrix Web Interface and Citrix Secure Gateway
* Creating, maintaining & monitoring Citrix farms (XenApp 6.5, PS 4.5)
* Documenting all the changes and updates made to the farm servers
* Performing monthly deletion of XenServer log files.

**INFOSYS | Century Link (Colorado) Snr. Network Security Engineer August 2018 – June 2019**

**Juniper Responsibilities**

* Member of a team of professionals responsible for analysis, maintenance, support, and troubleshooting in an enterprise LAN/WAN environment for Internet services access with direct client and third party.
* Team lead on Onshore/ Off Shore environment
* Technologies in network environment include but not limited to routers (BGP, Cisco ISR/ASR, Juniper, Alcatel), switches (Vlans, VTP, **Cisco catalyst)**
* Support Network Engineer for CenturyLinks for Starbucks activation that includes the design and implementation of Juniper SRX 300, EX 2200, Cradlepoints, Broadband Cables and circuits, IPSec and BGP
* Perform standard configuration, management, and maintenance tasks for Linux servers, requests, escalation support/ticket resolution and analysis in an enterprise LAN/WAN environment for datacenters, corporate, WAN links, and branch offices.

**F5 Big IP Responsibilities**

* Configuring and Implementing load balancing features to an in-production web server cluster
* Helping to bring the new F5 architecture online, test, and troubleshoot all configuration setting
* Implementing iRules from the vendor provided to maintain persistence based on session and for testing production environment
* Assisting in decommissioning the existing F5 appliances after migration
* Reviewed logs for all networking devices for unresolved abnormalities and problems and documented all server and network problems and other unusual events in details

**Cisco ASA/ISE**

* Integrating Configuring Cisco Wireless LAN Controllers WLC with ISE to perform Dot1x authentication for Wireless users.
* Configuring various Wireless authentications like **PEAP, EAP-FAST EAP-TLS** on **Cisco ISE**
* Configuring Administrating Dot1x RADIUS authentication for Wireless users and TACACS for Device Administration on **Cisco ISE**.
* Integrating Configuring **Cisco ASA** Firewalls with **ISE** to the Posture policy compliance perform CoA for remote **VPN IPSec, SSL AnyConnect** users

**Network Monitoring**

* Perform installation, configuration, customization for **SolarWinds** products on-site and remotely with clients globally.
* Implementation of NPM, NTA, NCM, FSM, and IPAM to manage and monitor network infrastructure, including routers, switches, firewalls, and load balancers on SolarWinds
* Design Groups and Dependencies to streamline monitoring and alerting.
* Review, update, and create network monitoring policies and procedural documentation.
* Manage **SolarWinds** NPM, WPM and IPMon monitoring services and nodes.

**CareerNation Network Engineer New York, 2015–2018**

**CareerNation** a global staffing, logistics company specializing in human resource, service and technology solutions for destination entry postal drop shipping within the direct mail industry. DLI also provides discounted shipping logistics solutions for non-mail, paper based products including printed material and raw print stock.

* Provided technical and vendor support services, designing and planning Network Planning, Implementing, Configuring, **SRX210, SRX240 Ex2200**
* Managed/mentored a team of engineers nationwide responsible for design, implemented, support and maintenance of network infrastructure (physical, logical and virtual) for various clients and environments.
* Knowledge and demonstrable experience of Security Information Event Management systems (Sentinel, Intel, **QRadar**, RSA, Splunk)
* Assisted with implementation of Windows Update Services server which greatly reduced administrator overhead for routine patching and security analysis duties
* Feature testing and automation of **Brocade 9850** series of data center router
* Tested Cisco IOS, IOS upgrades, configuration upgrades, implemented VLANS, Sniffers. Maintained the following **Cisco platforms 7600, 7500, 7200, 7000, 3560, 2900, 2801, 2000, ASA55XX, Catalyst 6500, 4500, 3560 and 2900.**
* Troubleshooting **IPSEC VPN Tunnel** related issues on PaloAlto firewall.
* Maintenance and configuration of policies on **PaloAlto** as per business requirement.
* Configuration and maintenance of new policies on **PaloAlto** firewall
* Perform **SIEM** product support and implementation
* Increased team productivity and automated repetitive tasks by using batch files**, PowerShell** and WMI.
* Specific engineering/troubleshooting activities including troubleshooting LAN/WAN connectivity including handling routers, switches, various WAN links (Frame Relay, TDM, LAN lines), monitoring/analysis and resolution of complex routing issues using various routing protocols including BGP, OSPF and EIGRP and acting providing technical mentoring/assistance to other technical team members and teams.
* Monitored and administered F5, RSA Security Analysis, Vulnerability Management, **Cisco and Juniper Firewall** to identify malicious activities
* Seasoned Systems Administrator familiar with **MS Windows 2000-2003 Server, 2000, XP OS**
* Additional responsibilities included proactive analysis, developing best practices, policies and procedures, reviewing analyzing Runbooks, MOP, network schematics including logical and physical diagrams.

**Siemens ICN Senior Network Engineer (TSE) Lagos, 2000–2014**

**Company Overview – Siemens ICN** Mobile offers a complete range of mobile solutions, including mobile devices infrastructure and applications. Is a fast growing business in a fiercely competitive, burgeoning wireless industry faced with the need for rapid product innovations and operations excellence. Senior management at this 29,000-person business unit of Siemens AG wanted to strongly link its strategic direction to everyday operations.

* Member of an enterprise network / telecom engineering team responsible end to end implementation of an enterprise nationwide network that included conducting site assessment, designing the implementation schematics/configurations, deploying the technologies, handling the advance configuration, testing and validating including hand off to the operations team for day to day support/administration.
* Acted as IT consultant and business analyst in improving and maintaining software systems across the firm, ensuring both data.
* Administration of **Win98, NT4, & Mac OS9; Cisco Catalyst 3500, 4000, 5000, 6500** series switches**; Cisco 2500, 2610, 7500 routers;** Sonicwall firewall with a familiarity with Pix 520, Local director, & Net Ranger Intrusion Sensor; cable network management
* Experience with large variances and model classes of **Cisco switches 2960, 4948, SG-200, Nexus7009and routers 2500, 2600, 1800, 2800, 2900, 4400**
* Involved in the support of **EX, SRX** routing products for Confidential
* Involved during p2-high troubleshooting on **SRX** forService provider network
* Contribution during the troubleshooting sessions on **SRX 100, 200, 300, EX 2200, 4200** platforms
* Worked on reviewing the bugs with **Juniper SRX, EX** switches
* Scheduled and allocated project activities, identified tools, standards, and guidelines suitable for the project.
* Provided risk management by monitoring the project schedule and quality.
* Reported project status regularly through emails and weekly meetings; formally tracked problems and issues to closure
* Additional responsibilities included Tier 3 support for any escalation support and acting as SME for major
* Hands-on experience with **PaloAlto firewalls** and a comprehensive knowledge of Policy.
* LDAP Synchronize with **Palo Alto firewall** and implement policy accordingly.
* Working knowledge on Cisco AnyConnect and **Palo Alto VPN’s**.
* change requests along with conducting annual technical audits to ensure proper functionality and compliance.
* Responsible for up to 150 servers and over 10,000 users in a global technology environment. **LINUX OS** supported web services, email, and a significant CRM application for this client*.*
* Experienced in many aspects of computer security technologies such as: **IDS/IPS**, port and vulnerability scanners, and network detection used in performance of daily activities and to perform assessments and audit
* Technologies in network environment included both voice/telecom and data network but not limited to routers, switches, security, firewalls, voice / collaboration (application, voicemail, email, text), wireless (GSM, access points, controllers, site surveys) and related technologies along with various server/application administration, system reimaging, and remote setup.