******Sushmitha Gangu**

**Senior Network Engineer (AWS, SDWAN, Security, Palo Alto, F5)**

**Phone: +1(260)222-8575**

**E-mail:**  **sushmitharg23@gmail.com**

**PROFESSIONAL SUMMARY:**

Experienced Cloud Communications and Network Professional working in medium to large scale environments, enterprise, and Data center networks. Expert in Routing & Switching, SDWAN Viptela, Network Security, Palo Alto, pfSense, Fortinet, Check Point, SonicWall Firewalls, Application Delivery, Wireless, Virtualization, SDN and Automation.

**CAREER HIGHLIGHTS:**

* Experience working in large-scale environments on high priority troubleshooting issues, several **Proof of concepts** for installations and Migrations to different vendor Equipment or implementing a new technology. Network Design, **IDF and MDF** architecture**, Datacenter Architecture,** and support roles, IOS upgrades, downtime procedures, Migration projects to different vendor equipment.
* Experience in Application Security Manager (**ASM**) which is a layer 7 web application firewall (**WAF**) available on F5's BIG-IP platforms.
* Working with **Akamai Kona WAF** and implementing http and https inspect rules for SQL injections, malicious file execution, cross site scripting.
* Expertise in installing, configuring, and troubleshooting **Juniper EX Switches** (**EX2200, EX2500, EX3200, EX4200, EX4500, EX8200 series).** Conducted query performance analysis in **Snowflake** to identify bottlenecks and optimize query execution times.
* Supported **Blue Coat** Proxy in explicit mode for users trying to access Internet from Corp Network.
* Working with **Ansible** and **Python** **Scripting** to automate configurations and Processes.
* Managed successful delivery of massive security response portfolio including **Splunk** and **Cisco ISE**.
* Configure and manage **LDAP** User management with **Checkpoint** Smart Directory. Implemented the policy rules and **DMZ** for multiple clients of the state on the Checkpoint firewall.
* Experience with cisco ACI and Arista Cloud Vision on a POC **Spine leaf Architecture** in Datacenter. I worked on **EVPN, VXLAN, VTEPS**, **Bridge Domains, MP-BGP etc**.
* Testing and validation of various **Wi-Fi hardware** products to ensure their quality and reliability.
* Experience on NSX VMware, **AWS**, Azure Etc. Participated in troubleshooting **SDN/SD-WAN** **Viptela** deployments.
* Proficient and high-level expertise using the F5 based profiles, **monitors, VIP’s, pools, SNAT, SSL offload, iRules, virtual Servers, iAPPs.** Migration experience from **ACE to F5**/ **old F5 to New F5.** Expert in **TMSH**.
* Experience with manipulating various **BGP** attributes such **as Local Preference, MED, Extended Communities, Route-Reflector clusters, Route-maps and route policy implementation**.
* Experience with **Panorama** M100 series and maintaining up to 23 firewalls in large networks.
* Working with **VSYS**, Security policies, App tags, **U-turn NAT**, Virtual routers, Zones, **URL** **filtering** using Domains, **SSL** decryption, **NAT** policies, monitoring, Panorama, APP ID on Palo Alto firewalls.
* Experience on **Amazon AWS** Virtual private cloud services.

**EDUCATION:**

* Bachelor ’s in Computer Science from **Osmania University, India**
* Master’s in engineering management with Information Systems from **Indiana Institute of Technology, USA**

**CERTIFICATION:**

* Cisco Certified Network Associate (CCNA)
* Cisco Certified Network Professional (CCNP)
* Palo Alto Certified Network Security Engineer (PCNSE)

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Networking Technologies** | LAN/WAN Architecture, TCP/IP, SD-WAN, VPN, VLAN, VTP, NAT, PAT, STP, RSTP, PVST, MSTP, CISCO ACI |
| **Networking Hardware** | Cisco Switches, Cisco Routers, ASA/ /Palo Alto/Fortinet/Juniper firewalls. |
| **Routing Protocols** | OSPF, ISIS, EIGRP, RIP, MPLS, IS-IS, BGP, Multicasting |
| **Security Technologies** | PAP, CHAP, Cisco, Blue Coat, Palo Alto, ASA, Fortinet, Checkpoint |
| **Network Monitoring & Management tools** | Snowflake, SolarWinds, Wireshark, HRping, WhatsupGold, Infoblox, Splunk, Nagios, ExtraHop Networks, FortiNDR, IronDefense, Obkio, CISCO ThousandEyes, NetBeez Network Monitoring, HPOV, ORION. |
| **Operating Systems** | Windows 10, LINUX, Cisco IOS, Cumulus, IOS XR, IOS-XE, NX-OS |
| **Routers** |  Cisco ASR 9000 Series, ISR 800 Series, ISR 1900 Series, ISR 2900 Series, ISR 3900 Series, and ISR 4000 Series, CISCO 1800, 2611,2800, 3600, 3845, 3900,4300, 4400, 4500, ASR 1000X, 7206VXR, Juniper M & T Series. |
| **Load Balancers** | F5 Networks (BIG-IP), NetScaler (Citrix), CISCO ADC |
| **Capacity & performance** | Cascade Riverbed (Flow Monitor), WAN Killer |
| **Switches** | CISCO 2960,3750,3850, CAT 9300, CAT9400, CAT 9500, 4500, 6500, 6800, Nexus 9K,7K,5K,2K, Arista cloud Switches  |
| **Programming Languages** | C, C++, Perl, Power Shell, Python, Yang, XML, Ansible |
| **Simulation Tools** | GNS3, VMware, OPNET IT GURU, OPNET Modeler, Cadence |
| **Firewalls** | Juniper Net Screen (500/5200), Juniper SRX (650/3600), ASA (5520/5550/5580), McAfee Web Gateway, Checkpoint, Palo Alto Firewalls. |
| **AAA Architecture** | TACACS+, RADIUS, Cisco ACS |
| **Features & Services** | IOS and Features, HSRP, GLBP, VRRP, IPAM IRDP, NAT, SNMP, SYSLOG, NTP, DHCP, CDP, DNS, TFTP and FTP Management, Open Stack, IVR’s, HLD and LLD documents, Dell equal logics |

**PROFESSIONAL EXPERIENCE:**

 **Client: ACLU, Broad Street, NY Aug’ 2024 – Till date**

**Role: Network Engineer**

**Project Description:** Managed multi-site network infrastructure with Cisco Meraki devices and Palo Alto firewalls, deploying secure Juniper MIST Wi-Fi, VPNs, and NAT rules. Centralized security and firewall policies using Panorama for streamlined operations.
**Responsibilities:**

* Supports Wi-Fi (Juniper Mist Access Points), wired networking (Juniper EX Series Switches), and SD-WAN (SRX Series Gateways).
* Managed and configured Cisco **Meraki** network devices, including switches and access points, through the centralized Meraki dashboard, streamlining network operations across multiple locations.
* Deployed secure Wi-Fi networks with **Cisco** **Meraki** access points, providing seamless guest access, bandwidth controls, and robust security features.
* Used **Cisco ACI** Fabric which is based on **Cisco Nexus 9000 series** switches and Cisco Application Virtual Switch (AVS). Designed, implemented, and maintained **AWS** backend infrastructure.
* Evaluated and tested **CISCO IOS XR** features on **Cisco NCS** routers to optimize network performance for service providers.
* Configuring access policies and security rules for **VXLAN**-extended networks.
* Deployed and integrated **FortiGate firewalls** into multi-vendor environments, ensuring secure connectivity across AWS, GCP, and on-premises networks.
* Multi-cloud transit architecture was configured and optimized using **Aviatrix** to improve connectivity and performance.
* Setting up **VXLAN-to-VLAN** gateways for seamless communication between legacy and VXLAN networks.
* Worked **DWDM** integration with **CISCO NCS** routers to support high-bandwidth optical networking.
* Integrated **CISCO NCS** routers with **SDN** controllers and automation tools like **Ansible/Python** to streamline network provisioning.
* Used **Python** (**Netmiko, NAPALM, Paramiko**) to automate configuration backups, interface checks, and route verification on Cisco and Juniper devices.
* Wrote custom **Bash scripts** to monitor link status, parse syslogs, and trigger alerts via email/SNMP traps.
* Developed **Python scripts** to pull real-time logs and security events from FortiAnalyzer using REST API and filter threat intelligence.
* Automated switch provisioning using **Python**/Ansible for pushing interface configs, QoS policies, and port descriptions.
* Maintained **Visio-based network diagrams** for enterprise infrastructure, improving documentation accuracy.
* Implementing and managing Aruba ClearPass for secure network access.
* Evaluate and incorporate leading **SD-WAN** solutions such as VMWare and Cisco SDWAN (Viptela), as well as tools like Aviatrix and SmartSite for network management.
* Configured **Juniper MIST** for Proactive optimization of wireless Devices performance
* Provided design and Contrail **SD-WAN** networking support using **Cisco ACI**, Cisco Wireless Controllers, Open-Stack, **Juniper** Contrail and Big Switch Networks LABs using Apple Configurator.
* Deployed zero-touch provisioning (**ZTP**) for branch offices, reducing deployment time and operational costs.
* Implemented Zero Trust Security Model (**ZTA**) to enhance access control and minimize attack surfaces.
* Responsible for the secure development of lifecycle environment from **NX-OS** to Application Centric Infrastructure (**CISCO ACI**) in Data center, implemented in the lab environment.
* Managed **Palo Alto’s** firewalls across multiple sites using Panorama. Creating Security policies with security profile enabled.
* Implemented and maintained **Palo Alto Prisma Access** cloud-delivered security for remote and branch users, enhancing secure access and reducing attack surface.
* Developed custom **ServiceNow** workflows for network request approvals and automation of routine tasks like port configuration and IP address assignment.
* Implemented **Aruba Wireless Controllers, Aruba Wireless Access Points** at corporate site as a part of WLAN Infrastructure.
* Worked on Routing protocols **EIGRP and BGP.** Working on **Infoblox** for **IPAM, DHCP and DNS**. Working on Linksys, SG500, Cisco, Arista switches and Cisco routers.
* Implementing and Maintaining Network Management tools (**Solar Winds, Zenoss, Infoblox, IPAM**)

**Client: Roche, New jersey Sep’ 2022 – Aug’ 2024**

**Role: SDN Network Engineer**

**Project Description:** Assisting product teams by gathering and analyzing data pertaining to Wi-Fi network performance, providing actionable insights for data-informed decision-making.Assisting in the migration from DMVPN to Cisco Viptela SDWAN, consisting of V-SMART controllers, V-BOND edge routers.

**Responsibilities:**

* Configured **SDN**-based WAN optimization using Cisco SD-WAN (Viptela) to enhance application performance and user experience across distributed locations.
* Developed and implemented security policy around the **Cisco ACS** (Authentication Control System), with **RADIUS** and **TACACS** authentication support against an Active Directory database, including device management, wireless and **VPN** applications.
* Configure and Maintain Authentication Services such as Alight **Cisco** **ACS** and **Aruba ClearPass** around the environment with troubleshooting AAA (**TACACS**+ & **RADIS**) services for users.
* Configure and manage Cisco routers and switches, including Catalyst, **Nexus**, or **Arista** EOS platforms, to facilitate efficient data transmission and network connectivity.
* Configured **Nexus 2000** Fabric Extender (FEX) which acts as a remote line card (module) for the **Nexus 5000** to connect servers and storage devices.
* Working on Cisco ISE and advanced technologies like **QOS**, Multicasting, **MPLS** and **MPLS-VPN** and **Bluecoat** proxy server SG.
* Integrated **EIGRP** with **MPLS** **on Cisco CSR 1000V** to provide scalable and efficient routing for virtualized environments.
* Implemented **FortiGate** 3000D with firmware version 6.4, utilizing **SSL** inspection, deep packet inspection, and advanced threat protection for robust network security.
* Automation using **iControl** and **Python v3** for configuration and backups in F5.
* Deployed, configured, and managed **Cisco Viptela SD-WAN** solutions for **WAN** connectivity, including integrating routers, switches **(Cisco ASR)**, **Juniper** **SRX**, and **Fortinet** firewalls to connect remote sites over the Internet.
* Demonstrated unparalleled expertise in **802.11** standards, including a/b/g/n/ac/ax, Wi-Fi security modes, Wi-Fi Mesh network, **Wi-Fi 6e**, and **Wi-Fi** performance parameters.
* Deployed, and maintained Fortinet security infrastructure including **FortiGate NGFWs, FortiManager, FortiAnalyzer, and FortiClient EMS** across multi-site enterprise environments, enhancing centralized policy control and threat visibility.
* Configured and optimized **FortiGate firewalls** for advanced threat protection, including IPS, application control, SSL inspection, antivirus scanning, DLP, and web filtering, reducing malware incidents by 45%.
* Integrated **FortiManager and FortiAnalyzer** for centralized configuration, real-time logging, event correlation, and compliance reporting, improving incident response time and audit readiness.
* Working with broadband technologies, including **DOCSIS** and DSL, as well as wireless technologies such as LTE, 5G, **802.11**ax (**Wi-Fi** **6**), and WPA3.
* Working with **Aruba and Cisco Wireless LAN controllers (WLC)**, Configuring and Provisioning AP’s, Virtual AP’s, RTLS, **Wireless** SSID’s, remote and campus AP’s, upgrading **WLC**, worked in Active/Active local Controllers and Master controller. Worked on **RAP3** for remote access.
* Quality Inspections and Operational Test (**OT**) events related to the 2GWLAN **Aruba** **Networks** Controllers, and Access Points (**Aruba 6000 controller**, Aruba AP65,70,124,85,125) system.
* Automation frameworks (**Terraform**, **Ansible**, **Chef**, **Puppet**) and automation scripts to support the Azure environment tools (Azure Resource Manager Templates).
* Designing a **Terraform** and deploying it in cloud deployment manager to spin up resources like cloud virtual networks, Compute Engines in public and private subnets along with AutoScaler in **Google Cloud Platform**.
* Work on **AWS** and **Azure** Cloud connectivity, Cloud Networking and Cloud security. Worked as an **Equinix** cloud Exchange provider.
* Managed **Docker** containers for efficient application deployment and utilized Kubernetes for container orchestration, including automated scaling and rolling updates.
* Configured **Kubernetes** network policies, load balancing, and service discovery to ensure secure, high-performance communication between microservices.
* Working on **Palo Alto** Firewalls, implemented Security Policies using ACL, Firewall, IPSEC, SSL VPN, IPS/IDS, AAA (TACACS+ & RADIUS).
* Work on **Google Cloud Platform** (**GCP**) services like computer engine, cloud load balancing, cloud storage, cloud SQL, stack driver monitoring and cloud deployment manager.
* Managed and administered **Juniper SRX and Checkpoint firewalls** across various zones (DMZ, Extranet, ASZ, and internal) anddeployed **Access, Distribution, and Core layers** in Data Center environments using **Juniper QFX and MX series switches.**
* Established **BGP** peering with external **ASNs** on **Arista 7500R** Series switches and implemented **BGP** route reflectors on **Cisco Nexus 7000** Series to optimize traffic flow, enhance network resilience, and streamline route advertisement within the AS.
* Configured and managed **Azure Active Directory** (AD) for user authentication, application access, and identity management.
* Implemented Spanning Tree Protocol (**STP**) optimization strategies to evenly distribute traffic and mitigate bottlenecks, enhancing network performance and reliability.
* Performed wireless site surveys using **Ekahau** tools and Sidekick to find the best access point placements, reduce interference, and improve Wi-Fi coverage.
* Configured **EIGRP** over **DMVPN** (Dynamic Multipoint VPN) on **Cisco ISR 4000** Series routers to enable secure and dynamic routing for remote sites.
* Conducted performance tuning and optimization on **Linux** systems, resulting in improved application response times.
* Configured and performed software upgrades on Cisco **Wireless LAN Controllers** (**WLC**) 5508 for Wireless Network Access Control (NAC) integration with **Cisco ISE**.
* **Implemented Cisco Meraki Enterprise Cloud Wireless Bridge/Repeater** to extend LAN across multiple buildings and **configured Meraki MX80, MX60 appliances** via **Meraki MX400 Cloud**.
* Implemented System for Cross-domain Identity Management (**SCIM**) integration to automate user provisioning and de-provisioning processes within **Snowflake**.
* Worked on **Zscaler** cloud proxies, supported migration from **IronPort** to **Zscaler**, and managed **ZIA** architecture with traffic forwarding via **GRE** tunnels, **Azure AD** authentication, and access policies using **ZCC 2.0**.
* Implemented **VMware** NSX Advanced Load Balancer (Avi Networks) for automated and scalable load balancing, ensuring high availability and performance for applications.
* Installed and configured Firepower Management Center 6.0 on **VMware**, integrated **ASA** Sourcefire Agents and Firepower **NGIPS** for monitoring, and configured **VMware** **NSX** **Edge** for routing, load balancing, and **VPN** services to enhance network flexibility and security.
* Configured Cisco **Software-Defined Access** **(SD-Access**) on Cisco Catalyst 9000 Series switches, enabling secure and scalable network segmentation.
* Combined **Bash with common Linux tools** (grep, awk, sed) for quick data extraction and report generation from network device logs and automated bulk device configuration changes by generating CLI commands within **Bash scripts** for Cisco and Juniper routers/switches.
* Monitored **OSPF** neighbor relationships and state transitions using **SolarWinds** Network Configuration Manager (**NCM**) for proactive troubleshooting.
* Utilized Cisco **DNA** Center’s path trace feature to visualize and troubleshoot end-to-end network paths, identifying bottlenecks and performance issues.
* Developed **Splunk** infrastructure and related solutions as per automation toolsets.
* Configured and managed **DHCP** services on **Cisco IOS** and Windows Server, including failover and redundancy, to ensure reliable IP address assignment and maintain network connectivity.

**Client: NWN Carousel, Atlanta GA Dec’ 2021-Sep’ 2022**

**Role: Network Security Engineer / NOC Engineer**

**Project Description:** Troubleshooting **L2** and **L3** Network Environments, performing installation, configuration, and deployment of **WAN** and **LAN** networking hardware, including the configuration and implementation of Routers, Switches and Firewalls. Customized ELK stacks to centralize log management, reducing incident response time by 25% and enhancing security monitoring.

**Responsibilities:**

* Worked on **Zscaler** policies, cloud app control policies, advanced threat, malware, sand box-based policies.
* Configure **IPSEC VPN** (Site-Site to Remove Access) and Maintain external Client Connectivity.
* Collaborated with cross-functional teams to define test plans for **Wi-Fi** hardware products, configured **WAN** connections with **Meraki** and **FortiGate SD-WAN**, and installed **Cisco Meraki** wireless access points **(MR66, MR18)** in warehouses.
* Configured and administered **Fortinet FortiGate 500D, 3000**, and **3815** series firewalls, including **ACLs** for network resource control, and integrated with **Forti Manager** for centralized policy management.
* Led a project to implement VPN solutions using IPSec and SSL VPNs for secure remote access; enforced device posture checks via **FortiClient EMS,** improving endpoint compliance by 60%.
* Network segmentation using **FortiGate VDOMs, VLANs**, and firewall policies to isolate critical infrastructure (PCI zone, guest networks), ensuring zero trust principles and regulatory compliance.
* Managed **Unix (AIX**) and **Linux** servers in a production environment, ensuring high availability, and configured **Citrix NetScaler ADC** and **F5** Load Balancers for traffic distribution and application availability. Led migration projects from **Citrix NetScaler** to **F5** across multi-site environments.
* Proficient in administering and troubleshooting both **Linux (Ubuntu, CentOS)** and **Windows Server** environments for network and security operations.
* Experienced in using **Linux CLI tools** (tcpdump, iptables, systemctl) and **Windows PowerShell** for automation and system management.
* Configuration and Administration of Alight Network Firewall to manage large scale firewall deployments, **Palo alto**, Cisco ASA-X Firepower, **Juniper SRX**, and Open-source **BSD** Firewalls.
* Configured **IPsec VPN** with multi-factor authentication (**MFA**) on **Palo Alto** Networks firewalls, enhancing remote user access security.
* Utilized **Jinja2** templating within Ansible playbooks to create dynamic and reusable network device configurations.
* Worked on upgrading **Aruba** controllers and Access points in troubleshooting the onboarding devices with the networks.
* Using automation tools like **Tufin** and **Riverbed** Net Profiler over Switches, Routers and Firewalls to discover, generate and deploy the Production configuration.
* Deployed **Silver Peak** Unity **Edge Connect** for **SD-WAN** and **WAN** optimization, utilizing dynamic path control, application acceleration, **WAN** hardening, and configured **Silver Peak** Orchestrator for centralized management and policy enforcement to enhance performance, security, and network operations.
* Deployed **FortiGate 6000 Series** NGFWs, configuring advanced security policies, intrusion prevention, and application control to safeguard against cyber threats.
* Configured multi-factor authentication (MFA) using **FortiToken** and **FortiToken** Mobile to enhance security for VPN and network access.
* Maintain network performance by using **SNMP** monitoring tools such as **SolarWinds** and **Omni Center** to perform network monitoring, analysis as well as troubleshooting network problems.
* Integrate Microsoft Active Directory (**LDAP**) into a checkpoint for identity awareness and user authentication.
* Implemented **OSPF** Fast Hello and Dead Interval on **Juniper MX480** routers to enhance network resilience and reduce failover time.
* Used Cisco **ACI** Fabric which is based on **Cisco Nexus 9000** series switches and Cisco Application Virtual Switch (**AVS**). Implemented, and maintained AWS backend infrastructure.
* Implemented Cisco ISE 1.2 for **Wireless 802.1x** Authentication and Authorization with Flex Connect
* Configured Cisco Unified Communications Manager (**CUCM**) to oversee and administer IP telephony systems, ensuring superior voice communication throughout the network.
* Implemented Quality of Service (**QoS**) policies on Cisco Catalyst switches to prioritize **VOIP** traffic, minimizing latency and ensuring consistent voice quality.
* Worked on the **Infoblox** DNS Traffic control, **DHCP**, and IPAM for Network control; Worked on the implementation of Domain Name Service.
* Worked on **Infoblox** to update the **DNS host** and A records to assist the part of the migration.

**Accenture, India Jan’ 2019 – Nov’ 2021**

**Role: Network Support Engineer / Network Engineer (Firewall, WI-FI, Wireless, WLAN)**

**Responsibilities:**

* Created documents for various platforms including **Nexus 7k**, ASR9k, and ASR1k enabling successful deployment of new devices on the network.
* Integrated **Blue Coat ProxySG** with Blue Coat Reporter to produce detailed reports on web usage, security incidents, and compliance, delivering comprehensive visibility and analysis.
* Used **Python** to parse text from device command outputs and generate basic network reports.
* Used **Bash** to schedule recurring tasks with cron for log cleanup and system monitoring.
* Worked on Cisco **ISE** deployment, which was a replacement for the **ACS** and provided new long-term and short-term guest wireless services for the Port Authority.
* Experience in Application Security Manager (**ASM**) which is a layer 7 web application firewall (**WAF**) available on **F5's BIG-IP** platforms.
* Performed upgrade process for **Cisco ISE** software from version 1.0.4 to 1.1 ADE-OS, patch management and data backup management.
* Configure and troubleshoot **Juniper** EX/SRX series switches.
* Performing network monitoring, analysis using various tools like **Wireshark**, & **SolarWinds**, Dynatrace, Extrahop tool helped for tracking root cause problems.