**PROFISSIONAL EXPERIENCE :**

Passionate Senior Network Engineer with 9 years of experience in data center refreshes, campus network upgrades, firewall and F5 installations, and network troubleshooting. Skilled in routing, switching, next-gen firewalls, load balancing, wireless technologies, and network security. Strong communicator, able to collaborate with all levels of the organization. A proactive team player who can also work independently to drive results and improve network performance.

**CAREER HIGHLIGHTS:**

* Senior Network Engineer with expertise in multiple client environments and diverse network technologies.
* Proficient in Switching, Routing, Firewalls, Network Security, Application Delivery Controllers, and Wireless technologies.
* Extensive experience in both campus and data center switching, including migration projects and architecture upgrades.
* Designed and implemented Cisco ACI in data centers, enabling container and cloud orchestration tools integration.
* Worked with Cisco Nexus 9000 NXOS and ASRs for MPLS in corporate settings.
* Familiarity with a wide range of network equipment, including Cisco, Juniper, Arista, Aruba, and Extreme switches.
* Configured Cisco Catalyst Switches for Dot1x support and integration with Cisco ISE.
* Strong expertise in Juniper Platform (QFX, EX, MX) installation, upgrade, migration, and troubleshooting.
* Experience with F5 load balancers and Citrix NetScaler for network monitoring, load balancing, and access policy management.
* Setup AWS Direct Connect for services like S3, EC2, and VPC, managing traffic flows between on-premises and AWS.
* Proficient in OSPF, MPLS, VLANs, FHRP, VPC, STP, port-channel, and various routing and switching protocols.
* Expertise in complex network environments, including security, load balancing, and wireless LAN controllers.
* Skilled in configuring and troubleshooting Juniper EX Switches and Cisco Routers.
* Worked with various routing protocols like OSPF, EIGRP, RIP, BGP, and MPLS.
* Configured F5 LTM for corporate applications and high availability, including APM and ASM modules.
* Proficient in VSS, VRF, VPC, VDC, and gateway redundant protocols (HSRP, VRRP, GLBP).
* Designed and implemented SD-WAN, SD-LAN, and WAN optimization solutions.
* Proficient in BGP attribute manipulation, including route policies.
* Extensive experience with Cisco ASA, Palo Alto, and Checkpoint firewalls.
* Worked with Bluecoat and McAfee Web Gateway Proxies for URL filtering and SSL decryption.
* Proficient in configuring and managing Aruba and Cisco Wireless LAN controllers.
* Integrated Cisco WLC with ISE for Dot1x authentication.
* Skilled in using network management tools like SolarWinds and Cisco Prime.
* Proficient in F5 configurations, including profiles, monitors, VIPs, and iRules.
* Experience with network troubleshooting tools such as ping, trace route, Wireshark, and TCP dump.
* Familiar with PPP, ATM, Frame-Relay, MPLS, and VoIP technologies.
* Expertise in NAT/PAT, access lists, security zones, and policies on SRX firewalls.
* Proficient in creating virtual servers and load balancing on NetScaler and F5.

**TECHNICAL SUMMARY:**

|  |  |
| --- | --- |
| **Network Configuration**: | Advanced switch/router configuration (Cisco IOS access list, Route redistribution/propagation). |
| **Routing Protocols**: | RIP, IGRP, EIGRP, OSPFv2, OSPFv3, IS-IS, BGP v4, MP-BGP |
| **WAN Protocols**: | HDLC, PPP |
| **Circuit switched WAN**: | T1/E1 – T3/E3/OCX (Channelized, Fractional & full). |
| **Security Technologies:** | Cisco FWSM/PIX/ASDM, Palo Alto, Cisco ASA, Checkpoint, Blue Coat proxy server. Port Security, DHCP Snooping, IP Source Guard (IPSG). |
| **Cisco Routers:** | Cisco ISR-1000, ISR-4000, ASR-1000, ASR-9000, ASR-5500, Meraki VMX 100. |
| **Redundancy and management**: | HSRP, VRRP, GLBP, RPR, NSF/NSR, STP, Wireshark, SolarWinds, SNMP |
| **Physical interfaces**: | Fast Ethernet, Gigabit Ethernet, Serial, HSSI, SONET (POS) |
| **Layer 2 technology**: | VLAN, VXLAN, HSRP, VRRP, GLBP, STP, RSTP, PVST+, MST, PVLAN, Optimizing STP (Port Fast, Uplink Fast, Backbone Fast, Root Guard, BPDU Guard), |
| **Layer 3 Switching**: | CEF, MLS, Ether channel (PAGP & LACP, Load Balancing) |
| **Switches**: | Catalyst 9400, 3850, 3650, 2960; Nexus 2k, 3k, 5k, 7k, 9k, Arista 7060X, 7260X, and 7320X, Juniper EX and QFX. |
| **Load Balancers:** | F5 LTM, GTM, Citrix Load Balancer. |
| **Network Management and Monitoring:** | Wireshark, Infoblox, HP OpenView, Cisco Prime, Splunk, Gigamon, Security Device Manager (SDM), Cisco Works; TCP Dump & Sniffer |
| **Scripting:** | Python, Ansible and TCL(F5), Golang. |
| **Ticketing Tools** | JIRA, CA Service Now |
| **Operating Systems**: | Microsoft XP/Vista/7, Windows Servers 2003/2008, Windows MS-Office**,** Microsoft project server 2013, Unix/Linux. |
| **Network Hardware/Platform** | Arista Network devices. |
| **Containerization** | Docker and Kubernetes |

**CERTIFICATIONS :**

* CCNA (Cisco Certified Network Associate)
* CCNP (Routing & Switching)
* Palo Alto Certified Network Security Engineer (PCNSE)

**EDUCATION:**

* Bachelor’s degree in Electronics and Communications Engineering from Vignan University (2011 to 2015).

**PROFESSIONAL EXPERIENCE:**

**Piramal Pharma Solutions, Sellersville, PA Jan 2023 – Dec 2024**

**Network Engineer**

**Key Responsibilities:**

* Conducted a comprehensive analysis of existing **Wi-Fi** infrastructure, identifying bottlenecks and coverage gaps. Developed a strategic upgrade plan, including selecting high-performance access points and collaborating in their placement across the site.
* Designed and implemented secure and scalable **VPC** (Virtual Private Cloud) architectures in AWS, utilizing subnets, route tables, and security groups to ensure efficient network segmentation and security.
* Utilized tools like Wireshark and **InSSIDer** to monitor and analyze Wi-Fi performance post-upgrade, fine-tuning configurations to maximize throughput and minimize interference.
* Implemented **VLAN** segmentation using Cisco switches, enhancing network security and traffic management. Managed Cisco routers with **BGP** for optimized external routing, ensuring redundancy and load balancing.
* Delivered end-to-end solutions in network design, engineering, implementation, and customer training.
* Configured Palo Alto firewalls with advanced security policies, **VPN** tunnels, and **IPS/IDS** systems, strengthening perimeter security.
* Planned and installed structured cabling, adhering to Cat6 and fiber-optic standards, increasing network speed and reliability.
* Designed and deployed **SD-WAN** solutions with Fortinet hardware, optimizing WAN traffic and reducing operational costs.
* Collaborated with senior engineers to redesign the network architecture, focusing on scalability and redundancy. Implemented **VLAN**s to segment network traffic and improve security.
* Involved in the revamp of old network architecture consisting of **Catalyst 3750** switches, which were replaced with Catalyst 9500, 9300, and 9200 switches. Collaborated in laying the new fiber cable for the entire site following the ring topology planned by architects.
* Upgraded core switches and routers to support higher data throughput and advanced features like Quality of Service (**QoS**) and Layer 3 routing. Configured Spanning Tree Protocol (STP) for loop prevention and failover.
* Deployed network monitoring tools such as **SolarWinds** to detect anomalies and ensure continuous network health. Implemented access control lists (**ACLs**) to restrict unauthorized access.
* Replaced old Polycom VVX 300 phones with **Yealink SIP T54W** phones and provisioned user profiles for those phones and deployed them to users.
* Led the design and implementation of a global network infrastructure that supports a pharmaceutical company’s research, manufacturing, and distribution operations, ensuring **high availability**, secure data transfer, and seamless connectivity across regions.
* Designed and implemented advanced **SD-WAN** solutions to optimize connectivity between the headquarters, global distribution centers, and research labs, improving application performance and ensuring seamless access to centralized applications across regions.
* Ensured network reliability and resilience by implementing multi-tier disaster recovery strategies, including cloud-based failover solutions and site-to-site replication, minimizing downtime and ensuring continuity of operations for critical business functions.
* Worked with cross-functional teams to design and implement advanced network segmentation strategies using micro-segmentation (**VXLAN**) to isolate sensitive systems such as clinical trials and regulatory data, preventing unauthorized access and ensuring compliance.
* Managed the deployment of edge computing solutions to support real-time analytics in pharmaceutical research, enabling faster decision-making and data processing without the need to send large datasets back to centralized servers.
* Oversaw the implementation of Zero Trust Network Access (**ZTNA**) for internal and external users, ensuring secure access to pharmaceutical research data, regulatory documents, and sensitive intellectual property, while mitigating the risk of cyber threats.
* Consulted with pharmaceutical compliance officers and legal teams to ensure that all network infrastructure met **FDA, EMA, and ISO** compliance standards, including secure data storage and transmission protocols.

**BlackRock, Dallas, TX Nov 2022 – Dec 2023**

**Senior Network Engineer**

**Key Responsibilities:**

* Led enterprise-wide network transformations for global organizations, consulting on the design and implementation of **SDN** (Software-Defined Networking) and NFV (Network Function Virtualization) for agility, scalability, and reduced operational overhead.
* Spearheaded 5G network rollouts, integrating **private LTE/5G** solutions and **MEC** (Multi-Access Edge Computing) for low-latency, high-bandwidth mobile applications, supporting **IoT** and real-time communications.
* Managed multi-vendor network infrastructures, integrating **Cisco**, **Juniper**, and **Arista** devices with SD-WAN solutions, ensuring seamless interoperability and unified network management.
* Architected and implemented zero-touch provisioning (**ZTP**) and self-healing networks, leveraging SD-WAN, Intent-Based Networking (**IBN**), and AI-powered automation to streamline network deployment and ensure uptime.
* Led the integration of cloud-native networking with **AWS Outposts**, **Google Anthos**, and **Azure Stack** to create hybrid and multi-cloud solutions, enabling organizations to scale their cloud infrastructure efficiently while maintaining network security.
* Worked on multi-cloud security models, implementing advanced **Zero Trust** security frameworks across public and private clouds using **Palo Alto Networks**, **Zscaler**, and Cisco Umbrella.
* Consulted on advanced **SD-WAN** architecture, incorporating application-aware routing, path selection, and traffic steering for optimal application performance, security, and cost savings.
* Developed next-gen virtualized network architectures using **VMware NSX**, **Cisco ACI**, and **OpenStack**, deploying micro-segmented networks for enhanced security in data center and cloud environments.
* Led the design of multi-site, high-availability architectures, using load balancing (**F5, Citrix ADC**) and geo-redundancy strategies to ensure business continuity in mission-critical applications and services.
* Orchestrated the end-to-end deployment of network services platforms (**NSP**s) for cloud-native applications, ensuring seamless integration of microservices architecture with networking layers.
* Implemented advanced traffic monitoring and data analytics to provide real-time visibility into network health, optimizing application delivery through **QoS, BGP** optimization, and traffic engineering.
* Led and contributed to network architecture reviews with key stakeholders to ensure design scalability, security, and performance for future growth, advising on the latest trends in **5G, IoT**, and cloud-native networking.
* Conducted network resilience and disaster recovery drills, **optimizing backup**, **failover**, and routing strategies to ensure continuous uptime in the event of network or service failures.
* Led cross-functional teams to execute large-scale network integration projects, working with stakeholders from cloud architecture, security, and operations to deliver seamless, integrated solutions.

**Verra Mobility, AZ May 2021 – Oct 2022**

**Network Security Engineer**

**Key Responsibilities:**

* Led the design and implementation of enterprise-scale network architecture, integrating **SD-Access** and **Cisco DNA** Center for simplified network management, policy enforcement, and automation.
* Architected and deployed multi-cloud networking solutions, leveraging **AWS** Transit Gateway, **Azure** ExpressRoute, and Google Cloud Interconnect to connect on-premise data centers with cloud environments.
* Managed the configuration and optimization of advanced firewall policies on **Palo Alto** and **Cisco Firepower** for highly secure edge and perimeter protection, including application-layer security, intrusion prevention, and **URL** filtering.
* Engineered advanced load balancing solutions with **F5 BIG-IP**, implementing global traffic management (**GTM**) and local traffic management (**LTM**) for **high availability** and **fault tolerance** in critical application environments.
* Deployed and optimized **Zscaler** Cloud Security for end-to-end secure internet traffic management, ensuring consistent security posture across distributed users and sites.
* Led the implementation of advanced network segmentation using micro-segmentation strategies (**VXLAN**, segment routing) to isolate and protect sensitive data traffic across data centers and cloud networks.
* Spearheaded the automation of network configurations using **Ansible**, **Python**, and **Terraform**, deploying infrastructure as code (**IaC**) for consistency, scalability, and faster provisioning of network resources.
* Implemented network performance monitoring and traffic analysis using **SolarWinds** Network Performance Monitor, NetFlow, and Wireshark, optimizing routing and load balancing for high-performance environments.
* Designed and implemented secure VPN solutions using **IPsec**, **SSL**, and **MPLS VPNs** to ensure secure connectivity for remote users and branch offices, while optimizing for bandwidth and latency.
* Deployed and managed Zero Trust Network Access (**ZTNA**) solutions, utilizing **Cisco ISE**, and Microsoft Intune for device authentication, access control, and secure user identity management.
* Collaborated closely with the cloud team to enable hybrid cloud networking, ensuring seamless traffic flow between on-premise data centers and cloud resources, optimizing both data residency and security compliance.
* Configured and managed **Advanced DNS and DHCP** solutions, ensuring dynamic IP allocation and DNS resolution for large-scale enterprise networks.
* Implemented network service chaining for SD-WAN environments, ensuring policy-based routing for multiple network services (firewall, load balancing, VPN) to improve agility and performance.
* Worked on next-gen security services, including **DDoS** mitigation with Cloudflare, **IDPS (Intrusion Detection/Prevention Systems), and SIEM (Security Information and Event Management)** tools to proactively detect and respond to threats.
* Conducted regular penetration testing and network vulnerability assessments to identify and mitigate security risks across network infrastructure, ensuring adherence to industry standards like **PCI-DSS and GDPR**.
* Led the development of disaster recovery strategies, designing site failover configurations, network backups, and business continuity plans to minimize downtime and data loss.
* Managed and supported the configuration and tuning of wireless networks, leveraging Cisco Meraki, Aruba Networks, and **Wi-Fi 6** technologies to ensure optimal coverage and security for large enterprise deployments.
* Provided in-depth network security training and mentoring for junior engineers, covering topics like network hardening, incident response, and best practices for network design and configuration.
* Designed advanced **QoS** policies to prioritize critical network traffic, ensuring high-priority applications (**VoIP**, video conferencing) received consistent, high-quality service.
* Played a key role in capacity planning and network scalability, leveraging **SD-WAN** and virtualization technologies to build networks capable of meeting future demands with minimal disruption.

**First Data, NY Oct 2019 - Apr 2021**

**Network Engineer**

**Key Responsibilities:**

* Led the implementation of SD-WAN solutions, optimizing **WAN** traffic routing and enhancing the resilience of the network by leveraging technologies like **Viptela** and Cisco **Meraki**.
* Configured and maintained advanced firewall security policies on next-gen firewalls (Palo Alto, Cisco Firepower), including intrusion prevention and secure **VPN** tunnels (**IPsec, SSL**).
* Deployed and configured load balancing for critical applications across **F5 Big-IP** to enhance availability, performance, and fault tolerance.
* Managed the configuration and optimization of **Zscaler** security policies, ensuring secure and seamless cloud access for remote users and branches.
* Worked with cloud-based networking solutions like **AWS Direct Connect** and **Azure Virtual WAN** to integrate on-premise networks with cloud infrastructure.
* Automated network monitoring and troubleshooting workflows using **Ansible** and **Python**, creating custom playbooks and scripts for routine configuration updates and incident response.
* Designed and deployed VLANs and VPN solutions for secure site-to-site communication across multiple geographical locations.
* Optimized Wi-Fi networks for high-density environments, performing **RF planning** and troubleshooting on **Cisco Meraki** and **Aruba** Networks access points.
* Implemented Network Access Control (**NAC**) solutions, using tools like **Cisco ISE** and **ClearPass**, to enforce device authentication and security policies.
* Deployed network segmentation techniques, utilizing **ACL**s, **firewalls**, and VLANs to segment sensitive traffic and protect critical infrastructure.
* Led troubleshooting for advanced network issues related to routing, load balancing, and security using tools like **Wireshark**, **NetFlow**, and advanced **syslog** analysis.
* Collaborated with the security team to deploy and manage security posture improvements, including **DDoS** mitigation and **Zero Trust policies**.
* Managed network performance reporting and analytics using advanced **SNMP**-based tools like **SolarWinds** Network Performance Monitor to deliver insights for network optimization.
* Contributed to the development of disaster recovery strategies by maintaining detailed network documentation, including **failover configurations**, security incident reports, and recovery plans.

**Microsoft, WA Oct 2017 - Sep 2019**

**Network Operations Engineer**

**Key Responsibilities:**

* Monitored network performance using **SNMP-based tools like SolarWinds and PRTG**, proactively identifying and resolving issues to ensure high availability.
* Performed real-time troubleshooting of network outages, analyzing logs, packet captures, and routing tables to identify and resolve root causes.
* Handled **Level 1 and Level 2 escalations**, diagnosing connectivity issues related to VLAN misconfigurations, interface errors, and routing loops.
* Assisted in configuring and maintaining **BGP and OSPF** protocols for WAN and data center interconnectivity, ensuring seamless network operations.
* Managed and troubleshot firewall policies and **NAT** configurations on Palo Alto, Cisco ASA, and Fortinet firewalls, assisting in rule optimization for security compliance.
* Monitored and supported load balancers (**F5, Citrix ADC**), ensuring optimal traffic distribution and application availability.
* Responded to security incidents by analyzing firewall logs, mitigating **DDoS** attacks, and escalating critical threats to the security team.
* Assisted in **Zscaler** policy enforcement, troubleshooting user access issues, and ensuring secure web traffic filtering across distributed environments.
* Provided L1/L2 wireless network support, troubleshooting **Wi-Fi coverage issues**, assisting in SSID configurations, and supporting enterprise-grade **WLAN** solutions.
* Automated routine network health checks using **Python** and **Bash** scripts to improve incident response times and reduce manual workload.
* Managed TAC cases with Cisco, **Palo Alto**, and other vendors to resolve hardware and software-related issues efficiently.
* Created and maintained network documentation, including topology diagrams, firewall rule change logs, incident reports, and resolution procedures to enhance team knowledge sharing.
* Implemented **ITIL-based incident management** best practices, reducing Mean Time to Resolution (**MTTR**) for recurring network issues.
* Provided training to **junior NOC** engineers on troubleshooting methodologies, **log analysis**, and escalation procedures for networking and security incidents.

**Liquid Hub, IND. Oct 2015 - Sep 2017**

**Role: Network Engineer**

**Key Responsibilities:**

* Configured IP addressing, subnetting, and **VLAN** segmentation to optimize network traffic flow.
* Deployed and configured Cisco routers and switches using **CLI**, implementing basic routing and switching protocols.
* Implemented static routes and inter-**VLAN** routing to enable seamless communication between different subnets.
* Created and applied basic Access Control Lists (**ACL**s) on routers to enhance security and control network traffic.
* Configured wireless access points (**WAP**s), defined SSIDs, and applied **WPA2** security for a secure wireless network environment.
* Set up SNMP-based monitoring tools (**PRTG, SolarWinds**) to track network performance and detect anomalies.
* Used diagnostic tools like **ping, traceroute**, and **Wireshark** to identify and resolve connectivity issues.
* Terminated and tested Ethernet cables, managed patch panels, and ensured proper cable labeling for efficient maintenance.
* Implemented switch security best practices, such as **port security**, disabling unused ports, and configuring MAC address sticky.
* Created detailed network topology diagrams and device configuration backups for reference and **disaster recovery planning.**