# A blue hexagon with white text Description automatically generatedA close-up of a logo Description automatically generatedSPURTHI

# [kotesh.benchsalesh@gmail.com](mailto:kotesh.benchsalesh@gmail.com" \t "https://mail.google.com/mail/u/1/" \l "label/UI+developer/_blank)

# SUMMARY:

* 8+ years of experience designing and securing enterprise/data center networks with a focus on scalability, high availability, and automation.
* Specialized in AdTech/OTT and real-time systems, optimizing networks for ultra-low latency using EVPN, VXLAN, and SD-WAN.
* Led cloud security transformations, migrating NSX to Azure and deploying AWS VPC/Direct Connect with Zscaler ZIA/ZPA for 5,000+ users.
* Automated firewall rule changes and SD-WAN provisioning with Python/Ansible, enabling dynamic BGP/OSPF validation.
* Built end-to-end automation workflows (Flask, Netmiko, Ansible Tower, MongoDB) across Cisco, Juniper, Palo Alto, and F5, cutting manual config by 40%.
* Developed Splunk + MongoDB log analytics pipelines to centralize telemetry, accelerating root cause analysis and proactive monitoring.
* Designed Spine-Leaf ACI fabrics with Nexus 7k/9k, supporting multi-tenant segmentation and greenfield datacenter rollouts.
* Deployed Next-Gen Firewalls (Palo Alto, FortiGate, ASA) with Panorama/FMC, ensuring policy consistency and regulatory compliance.
* Engineered F5/Citrix load-balancing architectures with SSL offload and iRules for zero-downtime deployments.
* Migrated from IronPort to Zscaler, integrated SCIM with Azure AD, and provisioned encrypted tunnels for cloud-based security.
* Created C/C++ and Bash diagnostic tools for custom packet capture and route validation, reducing outage troubleshooting times.
* Directed multi-vendor IOS upgrades & migrations, coordinating with NOC/PMO/vendor teams to ensure minimal downtime.
* Designed and managed wireless infrastructures (Aruba, Cisco WLC), implementing AP provisioning, SSID segmentation, and role-based policies.
* Architected AAA with RADIUS/TACACS+ integrated with Infoblox DNS/DHCP, supporting

**10,000+ endpoints** enterprise wide.

# CERTIFICATION:

* + Cisco Certified Network Associate (**CCNA**),
  + Palo Alto Certified Network Security Engineer (**PCNSE**).
  + AWS Certified Solutions Architect – Associate

# TECHNICAL SKILLS:

|  |  |
| --- | --- |
| **Routing & switching** | Cisco ISR/ASR, Catalyst (2K–7K), Nexus (2K, 5K, 7K), Juniper EX Series, Arista Switches; OSPF, EIGRP, BGP, IS-IS, HSRP, VRRP,  VLAN, STP, EtherChannel, IPv4/IPv6. |
| **Switching & Protocols** | Ethernet, LAN, VTP, PVST+, RSTP, Multi-Layer Switching,  802.1Q, Multicast, PAgP, LACP, CDP. |
| **Firewalls & Security** | Palo Alto NGFW (2K–5K), Check Point (R65, R80.x), Juniper SRX/SSG, Cisco ASA 5500 series, Fortinet; ACLs, NAT/PAT, VPN (IPSec/SSL), Port Security, AAA, IDS/IPS, HIPAA Compliance. |

|  |  |
| --- | --- |
| **Network Management and Monitoring** | SolarWinds NPM/NetFlow, Wireshark, Cisco Prime Infrastructure, Nagios, PRTG, Infoblox, HP OpenView, Splunk, Datadog. |
| **Load Balancers** | F5 BIG-IP LTM/ASM, Citrix NetScaler. |
| **Cloud & Automation** | AWS, Microsoft Azure, Cisco Meraki, Ansible, Python, Shell Scripting, Cloud Migration, SD-WAN. |
| **Operating Systems** | Windows Server 2012/2016, Linux, UNIX, Cisco IOS-XR, Nexus OS, MacOS. |
| **Wireless** | Cisco WLC/APs (1200 series), Aruba Wireless, Cisco Meraki Wi-Fi. |

**Professional Experience:**

**Shaw Industries, Dalton, Georgia**

**Sr. Network Security Engineer Sep 2024 - Present Key Contributions:**

* Installed and configured Palo Alto PA-5440/3420/5410 firewalls with IOC and Wildfire, strengthening malware prevention and advanced threat detection.
* Enforced Zero Trust by integrating Azure AD with RADIUS/AD, ensuring secure identity-based access across enterprise systems.
* Configured SSL decryption and forward proxy policies on Palo Alto firewalls, enhancing visibility into encrypted traffic and improving threat detection.
* Deployed Cisco ISE with 802.1X, dynamic VLANs, and segmentation, improving compliance and reducing unauthorized access risks.
* Reduced malicious site incidents by 40% through Akamai Secure Internet Access (SIA) DNS firewall integration across enterprise users.
* Designed and deployed Cisco Viptela SD-WAN with vEdge devices, cutting MPLS costs by 25% while enhancing branch-to-core routing resilience.
* Configured OSPF, EIGRP, and BGP on Cisco IOS routers, optimizing traffic distribution and improving failover convergence.
* Optimized BGP peering with ISPs and cloud providers (Azure/AWS), ensuring low-latency connectivity and resilient cloud access.
* Implemented Prisma Access to extend secure remote connectivity, enabling Zero Trust and encrypted access for hybrid workforce users.
* Expanded backbone connectivity with Cisco Nexus 7010/7018/5548/5600, integrating routers, firewalls, and load balancers across enterprise layers.
* Enhanced hybrid application delivery by integrating Cisco ACI with L4–L7 services, reducing troubleshooting times by 35%.
* Strengthened availability by deploying F5 BIG-IP r10600 appliances with cloud-based DDoS protection, securing applications against volumetric attacks.
* Tuned F5 GTM metrics to optimize DNS query handling and improve global traffic distribution across mission-critical workloads.
* Integrated Cisco SecureX with Palo Alto, F5, and SIEM tools, creating unified threat detection and response workflows.
* Automated backups, compliance checks, and anomaly detection with Python and Ansible, cutting manual workloads by 30%.
* Streamlined provisioning using Ansible Tower, Terraform, and Jenkins, ensuring deployment consistency and reducing errors.
* Proactively monitored bandwidth, device health, and security events with SolarWinds NPM/NCM, Infoblox DNS, and SNMP polling.
* Mentored junior engineers in SD-WAN, firewall, and automation best practices, driving knowledge transfer and improving team productivity.
* Developed SOC playbooks for firewall, SD-WAN, and DDoS incident response, improving MTTR (Mean Time to Resolution).
* Partnered with cross-functional teams to align SD-WAN and Zero Trust deployments with business confidentiality and compliance standards.
* Authored technical documentation, compliance reports, and network diagrams, ensuring audit readiness and operational continuity.
* Conducted quarterly PCI-DSS and SOX compliance reviews, remediating vulnerabilities and strengthening overall audit posture.

**Environments:** Palo Alto PA-5440/3420/5410, Cisco ISE, Cisco Viptela vEdge, Cisco ISR/ASR Routers, Catalyst & Nexus 7000/5000 Series, Cisco ACI, Arista 5000/7010X/7020R, F5 BIG- IP/GTM r10600, Akamai App & API Protector, Akamai SIA, Prisma Access, Cisco SecureX, SolarWinds NPM/NCM, Infoblox DNS, Ansible, Terraform, Jenkins, Python, ISEC, SNMP, OSPF, EIGRP, BGP, ACLs, QoS, Zero Trust, Hybrid Cloud Networks.

**CVS Health, Woonsocket, Rhode Island**

**Cloud Security Network Engineer July 2022 – July 2024 Key Contributions:**

* Configured AWS CloudTrail and CloudWatch pipelines to monitor API activity and integrate with SIEM dashboards, enabling anomaly detection and cloud-native security incident response.
* Automated compliance reporting and disaster readiness processes with Python scripting, improving audit preparation and ensuring alignment with corporate security frameworks.
* Implemented centralized multi-cloud log collection, integrating on-prem and cloud platforms to reduce blind spots and speed up threat investigation.
* Deployed and administered Palo Alto NGFWs (PA-5420/5220/7080) with IDS/IPS, SSL inspection, and advanced threat prevention for healthcare workloads.
* Utilized Palo Alto Panorama for centralized firewall management, ensuring governance, regulatory compliance, and standardized security policies across global sites.
* Led migration of global Check Point firewall infrastructure to Palo Alto, reducing operational risk and standardizing enterprise-wide firewall rulebases.
* Engineered FortiManager-driven administration of FortiGate appliances (100E/200E/500E/1800F), streamlining policy rollouts and cutting configuration errors by 25%.
* Strengthened threat detection with FortiGate Security Fabric and integrated threat intelligence services, reducing incident response times across distributed environments.
* Implemented Application Network Profiles (ANPs) in Cisco ACI, enforcing micro-segmentation and security baselines for sensitive healthcare and patient data workloads.
* Reviewed and optimized ACI security policies in collaboration with application teams, ensuring HIPAA-compliant access controls and reduced misconfigurations.
* Integrated F5 LTM 7000 reverse proxy with custom iRules to secure APIs, mitigate DDoS, and enforce protections against OWASP Top 10 vulnerabilities.
* Enhanced Zero Trust adoption by integrating Cisco ISE with Active Directory and SSO, enabling 802.1X access control and consistent endpoint policy enforcement.
* Deployed Cisco Viptela SD-WAN with vManage to secure branch-to-cloud connectivity, optimize encrypted traffic, and align with corporate SLAs.
* Expanded secure branch deployments with Meraki MX65/MX67 appliances, enforcing unified access policies and simplifying remote office rollout.
* Configured FMC-based IPS, URL filtering, and access policies to unify security enforcement across multi-vendor firewalls and distributed environments.
* Conducted HIPAA, PCI-DSS, and SOX compliance reviews, closing gaps and reducing audit findings by 35% through proactive remediation and hardening.
* Designed and tested backup, recovery, and business continuity procedures, ensuring disaster recovery objectives were met across critical workloads.
* Developed automation workflows using Python and Ansible for compliance checks and policy enforcement, reducing manual effort by 30%.
* Authored compliance playbooks, network diagrams, and technical documentation to support audits, knowledge transfer, and seamless project handovers.
* Mentored junior engineers on ACI micro-segmentation, VPN configuration, and cloud security practices, improving team capability and succession readiness.
* Implemented Splunk dashboards for real-time cloud security monitoring, integrating AWS, Azure, and GCP logs to improve incident visibility.

**Fifth Third Bank, Cincinnati, OH**

**Network Security Engineer March 2019 – June 2022 Key Contributions:**

* Administered Palo Alto NGFWs (PA-1410/450/5260/3430) and Check Point firewalls (R77, R80.x), creating and optimizing security policies, URL filtering, and threat prevention rules to protect online banking and transaction systems.
* Centralized management and compliance reporting through Palo Alto Panorama and Firepower Management Center, ensuring audit readiness for PCI-DSS and SOX frameworks.
* Deployed Palo Alto Prisma Access and GlobalProtect VPN with MFA, securing remote connectivity for 3,500+ users across retail banking branches.
* Designed and optimized FortiGate firewall deployments in 30+ branches, enabling resilient site-to- site VPNs and SSL inspection that reduced malicious traffic by 30%.
* Configured and maintained Cisco Catalyst (2900–7600) and ISR/ASR routers, integrating with

Juniper QFX5100 Layer 3 switches to modernize the bank’s core and branch networking.

* Implemented OSPF, EIGRP, MP-BGP, and RIP to enhance routing resiliency, support faster failover, and maintain high availability for ATM and mobile banking applications.
* Deployed F5 BIG-IP LTM appliances for load balancing banking applications, ensuring uptime and optimizing response times for high-volume customer transactions.
* Enforced east-west security policies in VMware NSX-T to secure hybrid workloads, supporting digital banking transformation and multi-tenant environments.
* Enhanced web application security with Blue Coat ProxySG and WAFs by enabling HTTPS inspection, ICAP filtering, and DLP features to protect against phishing and data exfiltration.
* Conducted root-cause analysis of security events and network slowdowns using Wireshark/tcpdump, improving troubleshooting efficiency by 25%.
* Led the migration of 50+ Cisco ASA firewalls to Palo Alto NGFWs with zero downtime, significantly improving detection and prevention of advanced threats.
* Implemented Cisco ISE for NAC (802.1X), securing wired and wireless endpoints and reducing risks of unauthorized device access across branches.
* Built detailed network diagrams, SOPs, and ITIL-aligned change documentation, streamlining audits and ensuring knowledge continuity.
* Monitored enterprise security posture using SolarWinds NPM/NCM, IDS/IPS logs, and SNMP polling, proactively addressing anomalies and optimizing bandwidth utilization.

**Environment:**

Palo Alto NGFW (PA-1410, PA-450, PA-5260, PA-3430), Panorama, Prisma Access, FortiGate, Check Point R77/R80.x, Cisco Catalyst 2900/3500/3700/7600, Cisco ISR/ASR, Juniper QFX5100, F5 BIG-IP LTM, VMware NSX-T, Blue Coat ProxySG/WAF, Cisco ISE, OSPF, EIGRP, MP-BGP,

RIP, VLAN, VxLAN, VPN (IPSec/SSL), Wireshark, tcpdump, SolarWinds NPM, ITIL, ServiceNow.

**Smart Recon, India**

**Network Support Engineer May 2017 – Aug 2018 Key Contributions:**

* Installed and configured software applications, antivirus, drivers, and security tools on end-user devices; performed troubleshooting for desktops, laptops, and peripherals.
* Configured and maintained TCP/IP, DNS, and DHCP network settings, ensuring adherence to company policies and standards.
* Assisted in configuring and verifying OSPF, EIGRP, and BGP under senior engineer guidance for inter-site connectivity.
* Implemented Response Policy Zones (RPZ) and upstream DNS firewalls to block malicious domains and enhance internet safety.
* Participated in backup and recovery procedures for network device configurations to ensure rapid restoration during outages.
* Configured Infoblox for DNS management, updated WAN configurations, and managed SSH network administration.
* Followed ITIL-based change management processes for network modifications to minimize downtime and ensure compliance.
* Used ServiceNow ticketing to log, track, and resolve incidents, service requests, and change approvals.
* Assisted in deployment and maintenance of Cisco Nexus 5548/7018/5600/7010, Catalyst 6500/3700, ISR, and ASR series devices, including VLANs, trunking, and interface configurations.
* Supported configuration and monitoring of Juniper SRX (320, 345, 380, 1500) firewalls to secure network access and reduce unauthorized connections.
* Monitored and assisted in the administration of Cisco WSA/CWS web security appliances to enforce browsing policies and block harmful content.
* Troubleshot network connectivity issues using ping, traceroute, and Wireshark, resolving outages within SLA timelines.
* Supported senior network engineers in network upgrades and hardware refresh projects, ensuring minimal downtime.
* Provided Level 1/Level 2 network support for an enterprise LAN/WAN environment with 500+ users across multiple branch offices.
* Monitored network performance using SolarWinds and produced capacity planning reports to identify and prevent bottlenecks.
* Configured and maintained VLANs, STP, and EtherChannel on Cisco switches to ensure redundancy, load balancing, and optimal Layer 2 performance.

**Environments:**

Cisco Catalyst (6500, 3700 Series), Cisco Nexus (5548, 7010, 7018, 5600), Cisco ISR/ASR Series, Juniper SRX (320, 345, 380, 1500), HP ProCurve, Dell Networking; OSPF, EIGRP, BGP, RIP, VLAN, STP, HSRP, VRRP, EtherChannel; Infoblox, Windows Server 2012/2016, Active Directory, Linux/Unix, VMware ESXi; SolarWinds, Wireshark, TFTP, PuTTY, ServiceNow, Cisco Prime Infrastructure; ACLs, Port Security, 802.1x, VPN (IPSec/SSL), DNS Filtering, RPZ; Cisco WLC, Aruba Wireless.