Avinash D
Senior Network Engineer
Email: davinashraj12@gmail.com
Contact: (737)-271-5397
LinkedIn: linkedin.com/in/avinashnetworks

PROFESSIONAL SUMMARY:

Senior Network Engineer with extensive hands-on experience supporting enterprise, data center, and hybrid cloud environments across **energy, healthcare, financial, and telecom domains**. Strong background in **Zero Trust security**, **SD-WAN**, **NGFW platforms**, **identity-driven access control**, and **high-availability networking**, supporting large-scale production environments and remote workforces.
Experienced with **Zscaler (ZPA/ZIA)**, **Palo Alto**, **Cisco**, **Fortinet**, **F5**, **Aruba**, and **Juniper** technologies, with deep involvement in **firewall policy management**, **routing stability**, **NAC integrations**, **wireless optimization**, and **cloud connectivity**. Skilled in automation using **Python and Ansible**, **proactive monitoring**, and **troubleshooting complex multi-vendor environments** while maintaining **security**, **performance**, and **uptime**.

CAREER HIGHLIGHTS:

• Hands-on experience implementing **Zero Trust access** using **Zscaler ZPA and ZIA**, securing remote and on-prem users through least-privilege, application-based controls.
• Strong hands-on exposure to **multi-vendor firewall platforms** including Palo Alto, Fortinet, Cisco Firepower/ASA, Check Point, Juniper SRX, and F5, covering policy enforcement, threat prevention, and traffic inspection.
• Practical experience implementing and supporting **SD-WAN solutions** using Cisco Viptela, Aruba SD-Branch, Versa, and Silver Peak to improve WAN resiliency and application performance.
• In-depth experience with **identity-based access control and NAC** using Cisco ISE and Aruba ClearPass, including 802.1X authentication, posture assessment, profiling, guest access, and MFA integrations.
• Hands-on involvement with **high-availability configurations** across firewalls, SD-WAN, and routing platforms, validating failover behavior and maintaining service continuity.
• Strong working knowledge of **enterprise routing and switching**, including BGP, OSPF, EIGRP, QoS, and Layer-2 resiliency mechanisms to support stable traffic flows.
• Practical experience configuring and optimizing **enterprise wireless networks** using Aruba and Cisco WLAN platforms, including Wi-Fi 6, RF tuning, WPA3 security, and high-density deployments.
• Hands-on exposure to **data center networking** using Cisco ACI, working with EPGs, contracts, service graphs, and policy-driven segmentation.
• Experience supporting **cloud networking across AWS, Azure, and GCP**, including VPC/VNet design, routing, firewall rules, VPN connectivity, and hybrid cloud integration.
• Hands-on experience implementing **cloud security controls**, including security groups, NSGs, cloud firewalls, and identity integrations aligned to least-privilege access.
• Experience improving operational visibility and reducing MTTR using **monitoring and analytics platforms** such as SolarWinds, Cisco DNA Assurance, FMC, Aruba AirWave, and SIEM tools.
• Automation experience using **Python, Ansible, REST APIs, and Ansible Tower** to standardize network and security operations and reduce manual configuration drift.
• Strong troubleshooting experience across **Layer 1 through Layer 7**, resolving complex network and security issues in multi-vendor production environments.
• Experience supporting **mission-critical networks** in compliance-driven environments, maintaining security, performance, and uptime.

CERTIFICATIONS:

- Cisco Certified Network Professional (CCNP)
- Cisco Certified Network Associate (CCNA)

- Palo Alto Networks Certified Network Security Engineer (PCNSE)
- Amazon Web Services Networking Specialty (AWS)

EDUCATION:

- Bachelor of Engineering in Electronics and Communication Engineering, India
- Master of Science in Computer Science, USA

TECHNICAL SKILLS:

Routing & switching	Cisco ACI (APIC), Cisco Nexus 9K/7K/5K, Arista EOS, Arista CloudVision, Cisco Catalyst 9000, Cisco Catalyst 3K/4K/6K, VRF, VLAN, VTP, VXLAN, EVPN, OSPFv2/v3, BGP, BGP FlowSpec, Route Reflectors, Traffic Shaping / DiffServ, EIGRP, MPLS, DMVPN, HSRP, VRRP, STP / RSTP / MST, Cisco DNA Center.
SD-WAN	Cisco SD-WAN (Viptela – vManage, vSmart, vBond), Versa Networks, Silver Peak Unity EdgeConnect, Cisco Meraki MX, Cisco SD-Access, Application-aware routing, AppQoE, DIA breakout, BFD-based failover, Auto-VPN.
Firewalls & Security	Palo Alto NGFWs (PA-3K/5K/7K, VM-Series, PAN-OS 9.x/10.x), Panorama, GlobalProtect, App-ID / User-ID, WildFire, Cisco ASA 5500-X, Cisco Firepower (FMC / FTD / NGIPS), FortiGate NGFW (FortiOS 6.x/7.x), FortiManager, FortiAnalyzer, FortiClient EMS, Check Point Firewall, Juniper SRX, IPS / IDS, SSL Inspection / Decryption, URL Filtering, DLP, WAF, DNSSEC, IPsec, SSL VPN, FortiWeb (WAF), F5 AFM, F5 APM, Cisco AMP, DDoS mitigation (BGP FlowSpec, F5 AFM).
Zero Trust & NAC	Zscaler ZIA, Zscaler ZPA, Cisco ISE, Cisco ACS, 802.1X, MAB, RADIUS, TACACS+, SAML, Azure AD, Aruba ClearPass (Policy, Profiling, Posture / OnGuard), ClearPass Device Insight, Dynamic VLAN Assignment, Posture Assessment, Illumio Adaptive Segmentation, CASB integrations, RSA SecurID, FortiToken / FortiToken Mobile.
Load Balancing & ADCs	F5 BIG-IP (LTM, GTM, ASM, APM, DNS, iRules, SSL Offload), F5 iControl API, Citrix NetScaler ADC (MPX / VPX, Gateway, GSLB, WAF), A10 Thunder ADC, VMware NSX Advanced Load Balancer (Avi Networks), GSLB, Content Switching.
Cloud Networking	AWS VPC, AWS Transit Gateway, AWS Direct Connect, AWS Security Groups, AWS NLB/ALB, AWS VPN Gateway, AWS CloudWatch, AWS CloudTrail, S3, VPC Flow Logs, Azure VNet, NSG, ASG, Azure VPN Gateway, Azure ExpressRoute, Azure Firewall, Azure Network Watcher, Azure Traffic Manager, Azure Bastion, Azure DDoS Protection, GCP VPC, Cloud NAT, Cloud VPN, Cloud Interconnect, Cloud Load Balancing, Cloud Armor,CloudDNS,VPCFlowLogs,Cisco NFVIS, Aviatrix Transit/FireNet/CoPilot, Equinix Cloud Exchange.
Automation & IaC	Ansible, Terraform (AWS, Azure, GCP, Aviatrix providers), Python (Netmiko, Paramiko, REST APIs, iControl, vendor SDKs), Ansible Tower, Git, GitLab CI/CD, Jenkins, Kubernetes Networking (Network Policies, Ingress, Service Load Balancing), Docker, Puppet, Chef, Cisco ISE REST APIs, Backup / Restore Automation.
Monitoring & Logging	SolarWinds NPM / NCM / IPAM / VNQM, FortiAnalyzer, Palo Alto Logs, Cisco FMC, Infoblox Reporting, Splunk Enterprise / ITSI / ES, Cisco DNA Assurance, Aruba AirWave, Riverbed SteelCentral, Zabbix (exposure), Wireshark, iPerf, SNMP v2 / v3, Syslog.
DDI & Web Security	BlueCat DDI, Infoblox NIOS, BIND, Windows DNS / DHCP, DNS RPZ, DNSSEC, Blue Coat ProxySG, Blue Coat CAS / Web Filter, Symantec ASG.
Wireless & Mobility	Cisco Catalyst 9800 WLC, Cisco WLC 5508, Cisco Aironet, Aruba 7200 Mobility Controllers, Aruba AP-535 / AP-555, ARM, ClientMatch, Aruba Wi-Fi 6, Cisco Meraki MR, Ekahau Site Survey / Pro / Sidekick, WPA2 / WPA3-Enterprise, Enhanced Open, 802.1X, Voice VLAN, DOCSIS, DSL, LTE, LTE, 5G.
Collaboration & Voice	CUCM, CUBE, SIP Trunks, Cisco IP Phones, Cisco Unity, VoIP QoS.
Security & Compliance	Nmap, Nessus, ITIL (Incident, Problem, Change, SACM), PCI-DSS, SOX, HIPAA, GDPR, SIEM workflows.

Tooling & Platforms	ServiceNow, NetBox, Confluence, Jira, Aviatrix CoPilot, Cisco Tetration, Citrix ADM, FortiSIEM.

PROFESSIONAL EXPERIENCE:

Avangrid Renewables - Clean Energy **Aug 2024 – Till Date**

Senior Network Engineer

Responsibilities:

• Automated **AWS** infrastructure deployments using **Terraform**, improving repeatability and reducing configuration drift across cloud environments.

• Integrated **Terraform** with **Ansible** and **Packer** to version, build, and configure **AWS** environments using repeatable **IaC** and configuration management workflows.

• Implemented **GCP** network security controls by configuring **GCP firewall rules** for VM ingress and egress governance and policy validation.

• Improved application performance using **GCP Cloud CDN**, enabling lower-latency delivery via cache locations and optimized content paths.

• Deployed **SD-WAN** using **Cisco Viptela** (ISR / vEdge) via centralized templates and policy-based routing, enabling application-aware path selection and branch resiliency.

• Implemented **SD-WAN** using **Versa** and **Silver Peak EdgeConnect**, leveraging analytics and dynamic path control to optimize user experience across multiple WAN transports.

• Designed and implemented **Palo Alto NGFW** platforms (**PA-3020 / PA-5050 / PA-7050**) delivering **App-ID**, **URL filtering**, and **Threat Prevention** standards aligned to business needs.

• Implemented **Fortinet** security architecture on **FortiGate 6000 / 3000D** (**FortiOS 6.4**) including **IPS**, application control, **SSL inspection / DPI**, and performance-tuned policies.

• Implemented **FortiGate HA** (active/passive and active/active) and validated failover and maintenance workflows to ensure continuous protection with minimal downtime.

• Deployed **Cisco ACI** fabrics (**APIC** with **Nexus 9000** ACI leaf–spine) to standardize policy-driven provisioning and accelerate application onboarding across multi-data-center environments.

• Executed phased brownfield migrations from legacy **L2 / L3** to **Cisco ACI**, including traffic-flow mapping, validation, and rollback planning to minimize downtime.

• Designed **ACI micro-segmentation** using **EPGs** and **Contracts** to isolate sensitive workloads and enforce least-privilege east–west controls.

• Built and operated **Arista EOS** fabrics with **CloudVision**, using configlets and telemetry for centralized configuration management and operational visibility.

• Implemented high-throughput **100G L3 leaf–spine** designs using **eBGP** on **Arista** (including **Arista 7500R** edge) to support data center consolidation and routing resiliency.

• Implemented **EVPN / VXLAN** underlay and overlay designs to enable scalable network virtualization, workload mobility, and multi-tenant segmentation.

• Implemented WAN and core routing on **Cisco ASR 9000** and **Juniper MX960**, applying **BGP** policies and communities to stabilize peering and optimize path selection.

• Scaled **iBGP** using route reflectors on **Nexus 7000** and edge peering on **Arista 7500R**, reducing session complexity and improving routing resiliency.

• Automated multi-vendor network operations using **Python** (**REST APIs**) and **Ansible**, standardizing configuration rollout patterns and reducing policy drift.

• Implemented proactive health-check automation by scripting CPU and memory monitoring and integrating alerts into operational workflows.

• Implemented **Zscaler Private Access (ZPA)** for 10,000+ remote users, configuring application segments, server groups, and least-privilege access policies across multiple data centers.

• Optimized **Zscaler Internet Access (ZIA)** using cloud app controls, advanced threat and malware protections, and policy tuning to balance security with user performance.

• Deployed **Palo Alto GlobalProtect v5.2** integrated with **Okta MFA**, tightening remote access posture and reducing credential-based risk.

• Migrated ADC services from **Citrix NetScaler** to **F5 BIG-IP** (**LTM / GTM / ASM / APM**), configuring VIPs, pools, health monitors, and packet capture for root-cause analysis.

• Implemented **AAA / NAC** using **Cisco ISE 2.6 / 3.0 (HA)** with **Catalyst 9300**, enforcing **802.1X** access policies and **TACACS+** for privileged device administration.
• Implemented **Aruba ClearPass 6.9** with **Aruba 5400R**, enforcing **802.1X / RADIUS** and role-based access for consistent wired and wireless segmentation.
• Designed high-density WLAN using **Cisco Catalyst 9800 WLC** and **Aironet 4800** access points, standardizing SSIDs and profiles to improve stability.
• Deployed **Aruba 7200 Mobility Controllers** (**ArubaOS 8.6**) with **Wi-Fi 6** access points (**AP-535 / AP-555**), validating coverage and capacity in high-density environments.
• Produced implementation documentation including **HLDs**, **LLDs**, **MOPs**, runbooks, and rollback plans to support repeatable changes and reduce outage risk.

Optum **Jan 2024 - June 2024**

Senior Network Security Engineer

Responsibilities:

• Built **Azure** network security constructs including **Azure Firewall**, **VPN** connectivity, route tables, **VNet** segmentation, and **Load Balancers**, validating flows end-to-end.
• Implemented **GCP** firewall policies by creating and validating ingress and egress rules controlling VM traffic aligned to least-privilege access requirements.
• Leveraged **GCP Cloud CDN** to improve content delivery performance and reduce latency through edge caching and optimized delivery paths.
• Integrated **Zscaler Internet Access (ZIA)** with **Azure AD** (**SAML**) and **SCIM provisioning**, automating user and group synchronization and enforcing AD group–based access policies.
• Designed and implemented **Check Point** and **Palo Alto NGFW** policies (**App Control / App-ID**, **URL Filtering**, **Threat Prevention**, **DLP / Data Filtering**) aligned to business requirements and risk posture.
• Owned **Check Point Firewall** operations across multi-tier environments, managing lifecycle rules, change control, and production verification.
• Built and maintained B2B and user VPN standards on **Cisco ASA 5520 / 5540**, delivering secure connectivity using **IPsec / IKEv2** with consistent encryption and authentication settings.
• Configured site-to-site and remote access VPNs on **Cisco ASA 5525-X** using **IPsec** and **SSL VPN**, supporting secure branch and remote user connectivity.
• Configured SSL decryption on **Cisco FTD 4100**, inspecting encrypted traffic to uncover hidden threats while applying performance guardrails and operational controls.
• Enabled **Advanced Malware Protection (AMP)** on **Cisco FTD 9300**, leveraging threat intelligence and sandboxing to improve zero-day detection and reduce malware spread.
• Deployed **F5 BIG-IP ASM 14.x (WAF)**, building policies to mitigate **SQLi / XSS** and tuning enforcement to reduce false positives while protecting critical web applications.
• Integrated **BIG-IP ASM 14.x** events into **SIEM** workflows, improving correlation of application-layer attacks and accelerating investigation and response.
• Configured **BGP** multipath on **Juniper QFX5100**, enabling **ECMP** load balancing and redundancy across parallel links for higher throughput and resiliency.
• Integrated **BGP** with **MPLS VPN** on **Cisco ASR 1000**, delivering scalable segmentation and routing isolation with consistent policy boundaries.
• Applied **BGP** path manipulation on **Cisco ISR 4451** (**AS-path prepending**, **MED**) to influence route selection and achieve traffic-engineering outcomes.
• Configured and troubleshot enterprise routing (**BGP / OSPF / EIGRP / RIP**) using route-maps, distribute-lists, and administrative distance tuning to control routing behavior during migrations and turn-ups.
• Integrated **Cisco ACI** with **VMware vSphere**, enabling automated network provisioning for virtual workloads with consistent policy enforcement.
• Configured **Cisco ACI Multi-Pod**, extending fabrics across data centers while maintaining centralized policy control and consistent segmentation.
• Optimized **Aruba WLAN** performance using **ARM** and **ClientMatch**, improving RF efficiency and roaming behavior through proactive channel, power, and client steering.

• Deployed **Aruba AirWave 8.2**, building dashboards and alerts for end-to-end wired and wireless visibility to reduce MTTR and support proactive operations.
• Expanded **SD-WAN** delivery across **Cisco Viptela**, **Versa**, and **Silver Peak EdgeConnect**, enabling application-aware path selection and improved branch resiliency across multi-transport WANs.
• Deployed **FortiManager 6.2** to centralize **FortiGate** policy control and firmware governance, improving consistency across multi-site firewall estates.

US Bank **Feb 2023 – Dec 2023**

Network Engineer

Responsibilities:

• Deployed **Palo Alto VM-Series (VM-300)** in **AWS** and **Azure**, extending consistent **NGFW** controls into cloud environments and aligning policy standards for hybrid governance.
• Integrated **SD-WAN** connectivity with **AWS** and **Azure**, optimizing access to cloud applications via secure, cloud-aware routing.
• Leveraged **Aruba SD-Branch** with **Zero-Touch Provisioning (ZTP)** and centralized management to streamline branch turn-ups and improve rollout consistency across distributed sites.
• Used centralized **SD-WAN controllers** (**Cisco vManage**, **Versa Director**) for template-based policy deployment, monitoring, and troubleshooting to improve operational efficiency.
• Configured **Zscaler Internet Access (ZIA)** for secure internet access across remote/mobile users, standardizing policy enforcement to reduce exposure while keeping performance consistent.
• Automated **ZIA** identity lifecycle using **Azure AD SCIM provisioning**, enabling user/group sync and consistent policy enforcement at scale.
• Designed **Cisco ISE** guest access portals with role-based access policies to deliver segmented, auditable visitor connectivity.
• Implemented dynamic **VLAN** assignment using **Cisco ISE**, enabling context-aware authorization based on identity and posture across wired and wireless access.
• Utilized **Cisco ISE** profiling to identify and classify endpoints, reducing manual exceptions through automated access enforcement.
• Deployed **Aruba ClearPass Device Insight** to identify and profile **IoT / BYOD** endpoints, improving visibility while reducing unknown-device risk.
• Automated device classification and enforcement via **ClearPass Device Insight**, applying device-type controls at connection time while minimizing manual **NAC** effort.
• Delivered **Cisco ACI L2 / L3** integrations by mapping legacy **VLAN / VRF** constructs into fabric policy and ensuring clean traffic flows during cutover and steady-state operations.
• Provided **L2 / L3** support for **Cisco ACI / APIC** including incident triage, fabric health checks, and post-change validation in production data center environments.
• Utilized **Cisco ACI APIs** to streamline configuration workflows and improve repeatability for data center policy operations.
• Integrated **Palo Alto PA-850** logs with **Splunk SIEM**, improving security visibility and speeding triage; used **Python** to streamline ingestion, normalization, and alerting workflows.
• Centralized **Palo Alto** administration using **Panorama 10.0** managing **PA-3200** class firewalls for unified policy deployment, change control, and security monitoring.
• Configured **Palo Alto WildFire 9.0** to strengthen zero-day protection via file/link analysis and automated prevention workflows.
• Enabled centralized **FortiGate** policy governance using **FortiManager**, standardizing rule deployment and reducing manual change risk across multi-site estates.

Amdocs **May 2019 – July 2022**

Network Engineer

Responsibilities:

• Configured and managed **Zscaler Internet Access (ZIA)** with advanced threat protection and URL filtering to block malware/phishing and reduce exposure to malicious destinations.

• Automated **ZIA** policy/configuration workflows to reduce manual effort and prevent configuration errors through repeatable, standardized changes.
• Implemented SSL decryption on **Palo Alto PA-220**, enabling encrypted traffic inspection while balancing privacy, performance, and compliance constraints.
• Automated **Palo Alto PA-3020** operations using **Ansible**, standardizing configuration deployments and reducing drift across firewall environments.
• Configured NAT policies on **Cisco ASA 5516-X**, supporting controlled access patterns and predictable translations aligned to security requirements.
• Implemented HA failover on **Cisco ASA 5545-X**, validating failover behavior to reduce downtime and improve operational reliability.
• Deployed **FortiWeb 6.3** as a **WAF**, creating and tuning policies/signatures to mitigate **SQLi / XSS / DDoS** with low false positives.
• Integrated **FortiWeb**, **FortiGate**, and **FortiAnalyzer**, enabling centralized monitoring and reporting and faster incident response for web attack events.
• Integrated **Cisco ISE** with **Firepower Management Center (FMC)** to correlate user and device identity context with threat events and improve investigation speed.
• Integrated **Cisco FTD** with **Cisco ISE**, enabling context-aware enforcement and improving segmentation accuracy using identity and endpoints.
• Configured **Aruba ClearPass OnGuard**, enforcing endpoint posture checks before granting network access to reduce risk from unmanaged or non-compliant devices.
• Integrated **ClearPass OnGuard** with AV, patch, and compliance systems, automating remediation workflows prior to granting elevated access.
• Integrated **Cisco ACI** with legacy infrastructure and built **ANPs**, enforcing application-specific policies at scale and improving segmentation consistency and policy governance.
• Integrated and stabilized routing across **Cisco Nexus 7000**, including **OSPF** virtual links, to maintain reachability across non-contiguous areas in complex OSPF designs.
• Performed deep **L1–L3** troubleshooting using **Wireshark**, producing targeted fixes based on packet-level evidence and traffic behavior.