Lavanya Katta | Sr. Network, Cloud & Cyber Security Engineer
E: lavanya.katta119@gmail.com | Ph: +1 (571) 789-8367

SUMMARY

Senior Network & Cloud Security Engineer with 6+ years of experience designing and securing mission-critical enterprise networks and hybrid cloud infrastructures across financial, telecom, and logistics sectors. Expert in multi-vendor firewalls (Palo Alto, Fortinet, Cisco, Checkpoint), load balancers (F5 BIG-IP/VIPRION), and cloud security (AWS/Azure).

Proven track record driving Zero Trust adoption, Illumio/Cisco ACI microsegmentation, and SD-WAN transformations. Adept in Python/Ansible automation for large-scale deployments, reducing errors and accelerating delivery by 60%. Recognized for leading firewall migrations, compliance-driven segmentation, and mentoring teams to build resilient, secure, and scalable infrastructures.

Certifications

- Cisco Certified Network Associate: Z6J5K8JFFC1EQJ91

TECHNICAL SKILLS

- **Firewalls:** Palo Alto PA-5220/3410/5410, FortiGate 3200F/100E/500E/1800F, Checkpoint R77.x, Cisco Firepower, ASA, Juniper SRX series
- **Routing:** RIPv2, OSPF, EIGRP, IS-IS, BGP, PBR, Redistribution, Route Filtering, Summarization, Static Routing
- **Switches:** Nexus 5k/7k/9k, Arista 5000/7050/7060/7500, Catalyst, Juniper switches
- **Network Management:** SolarWinds, Wireshark, SNMP, Tcpdump
- **Cloud:** AWS (EC2, VPC, IAM, S3, Route 53, ELB, EBS, Direct Connect, CloudFront, WAF), Microsoft Azure, ATT Net Bond
- **Load Balancers:** F5 BIG-IP LTM, VIPRION
- **Automation:** Python, Netmiko, Ansible Tower
- **Security Frameworks:** Zero Trust, PCI-DSS, SOX Compliance, NIST, CIS Controls

Professional Experience

R+L Carriers, Wilmington, OH

Sr. Network Security Engineer   **04/2024 – Present**

- Collaborated with compliance and audit teams to ensure firewall/SD-WAN policies aligned with PCI-DSS and SOX requirements, resulting in zero audit findings.
- Partnered with application owners and security teams to design resilient segmentation strategies, balancing performance with regulatory compliance.
- Configured and maintained Aruba wireless controllers running AOS 8/10 for enterprise networks.
- Performed firmware upgrades, feature configurations, and troubleshooting to ensure high network availability.

- Monitored enterprise wireless networks using Aruba AirWave, identifying and resolving connectivity and performance issues.
- Implemented guest access, BYOD policies, and compliance enforcement across enterprise networks.
- Administered cloud-managed wireless networks via Aruba Central, including device onboarding and configuration changes.
- Monitored network health, performance metrics, and firmware status across multiple locations.
- Managed network access control with Aruba ClearPass, including role-based access and device profiling
- Generated detailed reports on network health, client usage, and access point performance for IT teams.
- Deployed AWS Direct Connect with BGP routing, optimizing hybrid cloud traffic flows, improving throughput by 35%, and cutting inter-cloud transit expenses by 20%.
- Implemented and supported SD-WAN solutions by configuring overlay tunnels, application-aware routing, and centralized policies to improve performance and reduce WAN costs.
- Deployed SD-WAN across branch offices integrating with MPLS and broadband, ensuring high availability, secure VPN connectivity, and seamless cloud application access.
- Troubleshot SD-WAN edge devices, optimized QoS for critical applications, and automated configurations through orchestration platforms for large-scale environments.
- Automated deployments with Python/Ansible, cutting errors and saving 60% of engineering hours; built anomaly-detection scripts to flag traffic anomalies.
- Architected enterprise firewall modernization by deploying FortiGate 3700F/4400F/6300F clusters with FortiManager/FortiAnalyzer, enabling centralized policy governance and real-time threat analytics across 50+ branch and DC environments.
- Designed and implemented Palo Alto PA-7050/5430/5280 internet gateways with Panorama, standardizing VPN monitoring and reducing policy misconfigurations by 40% across the enterprise.
- Spearheaded Cisco ISE deployment (multi-site with Catalyst 9K/ASR 1K), enforcing 802.1X + certificate-based authentication and advancing the company's Zero Trust adoption strategy.
- Enhanced east–west security with Cisco ACI POD architecture and Juniper SRX 4300/4700 app-layer controls, reducing lateral movement risk across multi-tenant data centers.
- Engineered SD-WAN Viptela overlays and VXLAN fabrics on Arista 5000–7500 switches, enabling secure, application-aware routing and scaling branch connectivity by 40% without additional bandwidth costs.
- Implemented F5 VIPRION HA clusters for high availability and integrated AWS CloudFront + WAF to mitigate Layer 7 threats and protect customer-facing apps.
- Strengthened wireless security posture by deploying FortiAP access points integrated with FortiGate and Aruba controllers, improving secure branch connectivity for 10,000+ end users.
- Mentored junior engineers on automation and cloud networking best practices, raising overall team efficiency and reducing onboarding time for new hires.

Fidelity Investments, Boston, MA
Sr. Network Security Engineer   **09/2022 – 03/2024**
- Implemented Illumio microsegmentation across 3,000+ workloads, eliminating 70% of lateral movement pathways and satisfying PCI-DSS requirements.

- Architected AWS VPC security frameworks with custom routing, IGWs, and TGWs; integrated with F5 LTM for application delivery, achieving 99.99% uptime across high-traffic platforms.
- Orchestrated a multi-vendor firewall strategy with Palo Alto PA-5260/5450, FortiGate 100E–3200F, Cisco Firepower 3100–4200, delivering advanced threat prevention (IPS, URL filtering, malware sandboxing) and boosting detection by 30%.
- Streamlined troubleshooting and issue resolution through centralized cloud monitoring.
- Assisted in deploying new APs and network upgrades using Aruba Central dashboards.
- Configured authentication and authorization rules for secure Wi-Fi access using 802.1X and RADIUS.
- Coordinated with security teams to ensure adherence to corporate access policies.
- Used AirWave analytics to troubleshoot RF interference, client roaming, and bandwidth optimization.
- Assisted in network expansion planning by analyzing trends and network utilization metrics.
- Optimized controller settings for load balancing, roaming, and client performance across multiple sites.
- Implemented network policies to support secure and seamless wireless connectivity for employees and guests.
- Optimized DNS/DHCP posture by integrating Infoblox, reducing DNS incident response times by 30% through proactive detection.
- Secured enterprise access with Juniper SRX 4100/3800 firewalls integrated with Active Directory + MFA, supporting 20,000+ users globally.
- Designed ACI segmentation using Cisco Nexus 9800–9400 VXLAN fabrics, scaling to 1,200+ VRFs for multi-tenant workloads and enabling hybrid expansion.
- Led firewall migration projects consolidating legacy Cisco ASA/Checkpoint policies into Palo Alto Panorama, improving manageability and reducing legacy footprint.
- Deployed Aruba ClientMatch + Cisco Prime monitoring to improve wireless reliability and reduce connectivity drop-offs across trading floors and corporate offices.
- Collaborated with application, compliance, and DevOps teams to integrate Prisma Cloud security policies into CI/CD pipelines, ensuring secure workload deployments.
- Participated in cybersecurity tabletop exercises to validate incident response playbooks and reduce mean time to recovery (MTTR) in critical trading systems.
- Developed internal knowledge-sharing sessions and documentation to train teams on Zero Trust concepts, Illumio policies, and ACI-based segmentation, improving adoption across departments.

Comcast, Philadelphia, PA
Network Engineer   **05/2021 – 07/2022**
- Automated workflows with Netmiko, Python APIs (Cisco DNA Center, Juniper Contrail), and Ansible playbooks, improving configuration consistency and reducing deployment time by 50%.
- Integrated Cisco Firepower 1150/1120/4115 with Akamai WAF/DDoS mitigation, streamlining incident response and cutting threat response times by 25%.
- Ensured application resiliency with F5 BIG-IP LTM load balancing and refined ISEC compliance policies across multiple data centers.
- Managed Prisma Cloud workload security and enforced Cisco ACI tenant segmentation, enabling secure multi-cloud operations.

- Designed scalable traffic flows using VLANs/VRFs on Cisco ASR 9903–9906 routers + Nexus 9Ks, supporting high-volume multi-tenant traffic.
- Hardened enterprise edge with Meraki MX67–MX84 appliances and Juniper SRX 4700–5800, supporting branch offices and global connectivity.
- Integrated Akamai threat feeds into ticketing systems for faster SOC response and reduced false positives.
- Conducted traffic analysis with Wireshark/Tcpdump to troubleshoot high-volume application drops, identifying and resolving BGP flap issues.
- Worked with DevOps teams to integrate network automation tasks into release cycles, ensuring secure rollouts of microservices and APIs.

Tech Mahindra, India

Network Support Engineer   **07/2019 – 04/2021**
- Improved threat visibility by integrating ASA logs with Cisco Tetration, cutting detection time by 20%.
- Provided Tier 2/3 support for TCP/IP-based services (HTTP, FTP, SMTP, DNS) with a 95% SLA adherence rate.
- Resolved 95% of Tier 2/3 tickets within SLA, improving customer satisfaction scores.
- Configured and supported Checkpoint R80.x/R77.x firewalls, VPNs, and IDS/IPS solutions, ensuring reliable perimeter defense for client environments.
- Enhanced monitoring by integrating Cisco ASA 5520–5585 logging with Cisco Tetration for deep traffic visibility and anomaly detection.
- Improved routing performance with OSPF, BGP, RIP, and EIGRP tuning, ensuring stable connectivity across global enterprise networks.
- Administered Cisco TrustSec security groups, ACLs, and SolarWinds monitoring, improving real-time security insights and reducing false alerts.
- Conducted packet-level analysis using Wireshark to diagnose and resolve recurring issues in email and web proxy services.
- Worked closely with senior engineers during network migrations and firewall upgrades, gaining exposure to enterprise-scale transformation projects.
- Collaborated with global operations teams in Europe and North America, strengthening knowledge-sharing and incident response coordination.

Education
- M.S. in Telecommunications, George Mason University, Fairfax, VA
- Bachelors in Electronic and Communication Engineering, BVRIT, Hyderabad, India.