**Teja Sai K**

**Network / Security Engineer**

8128944538 • Email • [LinkedIn Profile](http://www.linkedin.com/in/teja-sai-ram-network-engineer)

**PROFESSIONAL SUMMARY**

* Result-Driven Senior Network & Security Engineer with over **6 years of experience** designing, implementing, and securing enterprise, healthcare, and service provider networks. Strong background in building **high-availability infrastructures** that support mission-critical applications, meet HIPAA and PCI requirements, and sustain **five-nines reliability** across global operations.
* Extensive expertise with **Cisco enterprise and data center technologies**, including **Catalyst 9300, 9400, 9600, ISR/ASR routers, Nexus 9K, ACI fabrics, DNA Center, and Viptela SD-WAN**. Skilled in deploying and managing **Palo Alto PA-Series firewalls, Fortinet FortiGate 6000F, Cisco ASA/Firepower, Arista EOS 7280R/7500R, Juniper MX960, F5 BIG-IP, Citrix NetScaler, and Aruba ClearPass/ISE**, ensuring secure, scalable, and high-performing network services.
* Proven ability to integrate **hybrid and multi-cloud environments**, establishing secure interconnectivity with **AWS Transit Gateway, Azure Virtual WAN, ExpressRoute, Direct Connect, and GCP Shared VPCs**. Experienced in **routing and security protocol optimization** including **BGP, OSPF, IS-IS, MPLS, VXLAN EVPN, IKEv2/IPsec, and SSL VPNs**, reducing latency and improving resiliency across complex topologies.
* Hands-on in **automation and Infrastructure-as-Code**, developing **Python scripts, Ansible playbooks, and Terraform modules** to standardize configurations, enforce compliance, and cut deployment times by up to **30 percent**. Skilled at integrating APIs and CI/CD pipelines with Git-based workflows to reduce manual errors and streamline enterprise-wide deployments.
* Recognized as a **dependable engineer during high-severity incidents**, trusted to restore services quickly, lead troubleshooting calls, and provide clear communication to both technical teams and business stakeholders. Known for **mentoring junior engineers, authoring runbooks, and driving best practices**, ensuring knowledge transfer and stronger operational discipline across teams.

**SKILLS**

|  |  |
| --- | --- |
| **Routing & Switching** | Cisco Catalyst 2960/3560/3750/3850/4500/6500, 9300/9400/9600, 8200/8300/8500; ISR/ASR Series (ISR800/1900/2900/3900/4300/4400, ISR1100, ASR900/920/9000); Cisco Nexus 3K/5K/7K/9K; Cisco UCS blades and UCS Central; Cisco vManage/vSmart/vBond; Arista EOS (720XP/7280R/7500R/7800, CloudVision); Juniper MX Series (MX5–MX2020), ACX7000, EX series; SRX/vSRX; Dell EMC S5248F-ON; HPE/Aruba switches; Cisco Meraki MS; IR1101/IR809 rugged routers |
| **WAN, Edge & SD-WAN** | Cisco Viptela ISR1100/8200, Catalyst 8500/8300 Edge, Cisco SD-WAN vManage, Versa FlexVNF, Silver Peak EdgeConnect, Meraki SD-WAN, MPLS L3VPN, Segment Routing, DMVPN, FlexVPN, GRE/IPsec, QoS (LLQ, CBWFQ, shaping, policing), OTV, VDC, vPC, MLAG, LISP; WAN optimization with Cisco WAAS and Riverbed SteelHead |
| **Firewalls & Security** | Palo Alto PA-Series (PA-220/3200/5200/7000, VM-Series), Panorama 10.x/11.x; Fortinet FortiGate 100D–6000F; Cisco ASA 5500-X; Cisco Firepower Threat Defense (FTD); Check Point R80.20/80.30; Juniper SRX/vSRX; Zscaler ZIA/ZPA; A10 Thunder TPS 4435; Symantec Blue Coat ProxySG; Illumio Adaptive Security; Akamai Kona Site Defender & Bot Manager; GlobalProtect VPN; SSL/TLS decryption; IKEv2/IPsec; SSL VPNs; NAC enforcement |
| **Load Balancers & ADCs** | F5 BIG-IP (LTM, GTM, ASM, APM, AFM, iRules/iApps), Citrix NetScaler MPX/VPX/SDX, A10 ADC, Cisco ACE, HAProxy, Loadmaster, NGINX Plus, Akamai CDN/WAF integration |
| **Wireless & Access Control** | Cisco WLC (5508/5520/9800), Cisco Meraki MR APs, Aruba 300/500 APs, Aruba Mobility Master, Aruba AirWave, Aruba ClearPass 6.x, Cisco ISE 2.x/3.x, 802.11 a/b/g/n/ac/ax, 802.1X (EAP-TLS/PEAP), BYOD and guest access, WPA2/WPA3 enterprise, Ekahau Pro/Sidekick surveys and RF heatmaps |
| **Cloud Networking & Hybrid Connectivity** | AWS (VPC, Transit Gateway, Direct Connect, Route 53, Security Groups, NACLs, CloudFront, ELB/ALB/NLB), Azure (vNet, VPN Gateway, ExpressRoute, Traffic Manager, Azure Firewall, Application Gateway), GCP (VPC, Interconnect, Shared VPC, Cloud Router, Cloud Armor), VMware NSX-T and NSX-V, VMware Cloud on AWS, Cisco ACI (Multi-Pod, APIC), Hybrid WAN and interconnect design across AWS, Azure, and GCP |
| **Automation & Infrastructure-as-Code** | Python (Netmiko, NAPALM, Paramiko, Boto3, PyATS, RESTCONF/NETCONF APIs), Ansible (playbooks, Tower/AWX, Jinja2 templates), Terraform (AWS, Azure, GCP, Palo Alto), Jenkins CI/CD, Git/GitHub version control, YAML/JSON scripting, NetBox CMDB automation, Infrastructure compliance enforcement |
| **Monitoring & Management Tools** | Infoblox IPAM, BlueCat BAM/BDDS, Cisco Prime Infrastructure, Cisco DNA Center Assurance, SolarWinds NPM/NCM/NTA, Splunk Enterprise & Splunk ES, Splunk Phantom/SOAR, Wireshark/tshark, vManage Analytics, Versa Director, Arista CloudVision, ThousandEyes, PRTG, Nagios, LogicMonitor, Datadog, ManageEngine OpManager, Zabbix, SevOne, NetFlow Analyzer, Icinga, Foreman, Rackspace Monitoring, Cribl Stream/Edge, Auvik, ServiceNow ITSM |
| **Data Center & Virtualization** | Cisco ACI (APIC, Multi-Pod, Tenant/VRF/BD provisioning), Cisco UCS blades and UCS Central, VMware vSphere/ESXi/vCenter, VMware NSX-T and NSX-V microsegmentation, Nutanix HCI and Prism, Hyper-V, Dell EMC Isilon/VMAX, NetApp ONTAP, SAN/NAS storage, Fibre Channel zoning, VMware Horizon VDI, VMware HCX migrations, Converged Infrastructure stacks |
| **Protocols & Standards** | TCP/IP, IPv4/IPv6 dual-stack, RIP, EIGRP, OSPFv2/v3, BGP-4, IS-IS, MPLS (TE, L3VPN, Segment Routing), VXLAN EVPN overlays, Spanning Tree (STP, RSTP, MST), EtherChannel (PAgP, LACP), HSRP, VRRP, GLBP, NAT/PAT, DHCP, DNS, IPAM, QoS (classification, shaping, policing), SNMPv2/v3, Syslog, 802.1Q VLAN tagging, AAA, TACACS+, RADIUS, 802.1X authentication, TrustSec, microsegmentation policies |
| **Operating System** | CAT IOS, IOS XE, XR, NX-OS, Junos, PANOS, F5 BIGIP OS, Linux, Windows  |

**CERTIFICATION**

Cisco Certified Network Associate (CCNA)

Cisco Certified Network Professional (CCNP)

Palo Alto Certified Network Security Engineer (PCNSE)

AWS Certified Advanced Networking – Specialty (ANS-C01)

**PROFESSIONAL EXPERIENCE**

Network Engineer

AT&T - Dallas, TX 01/2025 - Current

* Configured and maintained **Cisco ISR1100 and Catalyst 8500/9300X/9400X/9600** platforms via **Cisco vManage 20.x**, developing policy-based templates for QoS, ACLs, and SLA tracking; integrated **Azure Virtual WAN** over BGP/IPsec tunnels to 150+ branches, stabilizing hybrid WAN circuits and reducing packet loss by **18%**.
* Coordinated hybrid WAN migrations with **cloud architects, security engineers, and carriers**, documenting change windows and fallback procedures; ensured zero downtime during cutovers while improving resiliency for **mission-critical SaaS workloads**.
* Designed and enforced **App-ID, WildFire, SSL Decryption, and User-ID** policies on **Palo Alto PA-220/3200/5200 firewalls** managed via **Panorama 11.x**, eliminating blind spots in encrypted traffic and improving threat detection accuracy by **22%** across 10,000+ daily sessions.
* Hardened remote connectivity by implementing **IPsec VPNs, NAT policies, and SSL decryption**, which lowered unauthorized access attempts by **17%** while supporting **1,200+ concurrent VPN users**.
* Administered **Fortinet FortiGate 6000F appliances** with **FortiClient EMS** integration, applying IPS, URL filtering, and endpoint compliance posture checks; maintained alignment with AT&T’s **zero-trust access strategy** across a 1,500-device fleet.
* Led the replacement of legacy **DMVPN/IPsec hubs** with **Versa FlexVNF and Silver Peak EdgeConnect**, applying traffic steering, QoS, and FEC; improved **Office365 and WebEx throughput by 30%** and reduced site-to-site latency by 20–30 ms.
* Configured **Cisco Viptela ISR1100 and Catalyst 8500 SD-WAN** edges via vManage, automating template deployment, enabling BGP/OSPF dual-homing, and building redundant IPsec tunnels; achieved **sub-second failover** and seamless SaaS access.
* Assisted in Versa FlexVNF branch onboarding, applying **dynamic path control (DPC)** and **Bidirectional Forwarding Detection (BFD)**; sustained WAN uptime during carrier outages and reduced mean outage duration by **14%**.
* Proactively monitored WAN health with **vAnalytics and Versa Director**, generating utilization baselines and escalating circuit degradation events; reduced **MTTR for provider escalations by 20%**.
* Automated **VRF, tenant, and bridge-domain provisioning** within **Cisco ACI Multi-Pod** and **Arista EOS fabrics** using **APIC REST APIs and Python scripts**, cutting configuration turnaround time by **23%** and ensuring compliance with naming standards.
* Configured **L3Out routing** across **Cisco Nexus 9300/9500, Arista 7280R, and Juniper MX960** platforms, optimizing OSPF/BGP redistribution and route summarization; reduced routing convergence times by **15%** during failovers.
* Investigated **routing adjacency flaps, MTU mismatches, and interface CRC errors** on **Juniper MX960** platforms, using CLI counters and sFlow; restored stable peerings and improved backbone reliability across 40 Gbps links.
* Deployed **Cisco SD-Access fabric** via **DNA Center 2.x** with **Cisco ISE 3.x**, implementing TrustSec SG-tags, dynamic VLAN assignments, and endpoint profiling; achieved **19% higher compliance rates** in security audits.
* Tuned SDA underlay protocols (**IS-IS, BGP, LISP**) to sustain **98% successful roaming rates** for 8,000+ wireless endpoints across campus and branch environments.
* Integrated **Aruba ClearPass 6.11** with RADIUS/LDAP for NAC, applying role-based profiles for corporate staff, IoT, and guest access; reduced rogue device connections by **22%**.
* Configured **TACACS+ policies on Cisco ISE**, enforcing role-based CLI access for 150+ engineers; maintained full command logging, which reduced **unauthorized changes by 18%**.
* Supported load balancing and security for web apps using **F5 BIG-IP i5800 LTM/GTM/ASM/APM** and **Citrix NetScaler MPX appliances**, enabling SSL offload, WAF protection, and HA failover for customer-facing portals.
* Performed SSL/TLS certificate upgrades across **F5 and Palo Alto appliances**, enforcing **TLS 1.3-only ciphers**; passed external PCI/DSS compliance audits without findings.
* Developed **Python/Ansible playbooks** leveraging Netmiko, NAPALM, and Jinja2 templates, integrated into **Jenkins pipelines** with Git-based version control; reduced misconfigurations by **28%** and accelerated rollout cycles.
* Automated **Infoblox DNS/DHCP/IPAM** management through REST APIs and Ansible playbooks; streamlined address allocations, reduced manual data entry, and improved IPAM accuracy by **40%**.
* Authored **Terraform modules** to build AWS VPCs, Azure VNets, and GCP Shared VPCs with integrated firewalls, NAT gateways, and route tables; cut cloud provisioning time by **35%**.
* Delivered hybrid-cloud resiliency using **AWS Transit Gateway, Direct Connect, Azure Traffic Manager, and GCP Interconnect**; maintained **99.8% availability** for multi-cloud WAN interconnects.
* Hardened **Google Cloud Shared VPCs** with least-privilege firewall rules, IAM controls, and service project isolation; improved inter-service traffic security by **14%**.
* Installed and configured **Dell EMC PowerSwitch S5248F-ON** ToR switches in data centers, enabling VXLAN overlays, LACP uplinks, and BGP peering; boosted throughput by **12%** for virtualization clusters.
* Integrated **VMware NSX-T** microsegmentation and distributed firewall rules with Cisco ACI policy groups, reducing lateral threat movement and achieving **zero trust segmentation**.
* Authored detailed **runbooks, topology diagrams, and SOPs** for SD-WAN, ACI, and firewall operations; mentored junior engineers during incident resolution and reduced escalations by **25%**.

Network Security Engineer

UHG/OPTUM - Hanover Park, IL 01/2024 - 12/2024

* Engineered end-to-end deployments of **Palo Alto PA-Series firewalls (PA-220, PA-3200, PA-5200, PA-7080)** and **VM-Series** in hybrid environments, implementing HA pairs and failover testing; enforced App-ID, SSL Decryption, and GlobalProtect VPNs, reducing security incidents by **15%** across 5,000+ endpoints.
* Optimized firewall posture using **User-ID, Content-ID, and advanced threat prevention**, leveraging DNS Security and WildFire; successfully blocked malware callbacks and lowered false positives by **20%** in SOC alerts.
* Configured **GlobalProtect VPN** with **LDAP, RADIUS, and SAML-based MFA**, providing secure remote access for **1,000+ clinicians and staff**, ensuring HIPAA-compliant remote connectivity.
* Centralized administration via **Panorama 10.x**, building shared device groups, pushing hierarchical security policies, and generating compliance reports; reduced manual effort in multi-site policy deployment by **35%**.
* Led firewall migrations from **Check Point R80.20, Cisco ASA 5500-X, and Fortinet FortiGate 3000** to Palo Alto NGFWs, performing phased cutovers, policy translation, and rollback planning; achieved **zero downtime** across 12 hospitals.
* Directed proxy migration from **Symantec Blue Coat ProxySG** to **Zscaler ZIA/ZPA**, integrating SAML-based identity and SSL inspection; successfully transitioned to **Zero Trust Web Access** for 18,000+ healthcare staff.
* Administered **BlueCat BAM/BDDS DNS/DHCP/IPAM**, provisioning segmented VLANs for EHR apps and IoMT devices; ensured full HIPAA compliance and sustained **99.99% uptime** for name resolution services.
* Integrated **Splunk Enterprise Security** with Palo Alto firewalls, Blue Coat logs, and F5 appliances to enable correlated threat detection; reduced **MTTR for incident investigations by 27%**.
* Applied URL filtering, SSL interception, and HIPAA-aligned DLP controls, preventing PHI leaks and blocking malicious sites; increased compliance audit pass rates by **19%**.
* Configured **Arista 720XP/750 Series switches** with IKEv2 VPNs, NAT, and SSL VPNs, segmenting critical workloads; improved throughput across WAN links by **12%**.
* Assisted in deploying **Cisco ACI Multi-Pod** with **Nexus 9500 spine / 9300 leafs**, creating VRFs and bridge domains to support EMR workloads improved east–west performance by **15%**.
* Integrated **Cisco ACI with VMware vCenter**, automating endpoint group mapping to VM tags, which reduced provisioning time for medical applications by **30%**.
* Assisted in rolling out **Cisco DNA Center** to automate WLAN/LAN provisioning across clinics; implemented config compliance templates and enabled **faster onboarding for 50+ sites**.
* Deployed **Aruba ClearPass 6.11** and **Cisco ISE 3.x**, enabling 802.1X EAP-TLS NAC with posture enforcement; securely onboarded IoMT and contractor devices, cutting rogue connections by **22%**.
* Hardened perimeter with **A10 Thunder TPS 4435** and aFlex rules, mitigating SYN floods and volumetric DDoS attacks; maintained 100% uptime during attack simulations.
* Managed **F5 BIG-IP i5800 (LTM/GTM/ASM)** clusters, configuring ASM signatures to mitigate **OWASP Top 10 threats**; enabled application resiliency for patient portals.
* Automated SSL/TLS certificate renewal workflows using **Ansible, TCL iRules, and HashiCorp Vault**, eliminating expired cert outages and cutting renewal time by **40%**.
* Built **Ansible 2.12 playbooks with Netmiko/NAPALM** to automate switch and firewall configs across 100+ devices; eliminated config drift and reduced engineer workload by **25%**.
* Developed **Python scripts** integrating Palo Alto XML API and Splunk REST API, achieving near real-time alerting for IOC matches and improving threat response time by **35%**.
* Automated **tenant, VRF, and segment creation** in **Arista CloudVision** across 7280R/7500R chassis via REST APIs; accelerated multi-tenant deployments by **30%**.
* Provisioned multi-cloud VPCs in **AWS, Azure, and GCP** using **Terraform**, including firewall policies, route tables, and VPN gateways; reduced manual provisioning time by **35%**.
* Deployed **AWS Direct Connect Gateway with BGP/IKEv2**, tuned **Route 53 latency-based failover**, and configured Azure VPN gateways; ensured high availability for EMR cloud workloads.
* Optimized wireless infrastructure using **Aruba 300/500 APs** with AirWave, ClientMatch, and **Ekahau Pro/Sidekick surveys**; ensured reliable coverage for IoT medical devices and raised Wi-Fi reliability by **21%**.

Network Support Engineer

Websoft Technology PVT LTD 07/2019 - 07/2023

* Optimized VLAN segmentation and inter-VLAN routing on **Cisco Catalyst 3560, 3750, and 4500 Series switches**, configuring 802.1Q trunking, VTP pruning, and DHCP snooping; improved LAN segmentation, reducing broadcast storms and cutting security incidents by **20%**.
* Configured **EtherChannel with LACP/PAgP** and Spanning Tree enhancements (RSTP, MST, BPDU Guard, Root Guard) across multi-switch topologies; increased LAN stability and reduced downtime by **15%**.
* Tuned root bridge elections and adjusted path costs to balance load across redundant uplinks, achieving predictable traffic flows and higher availability in multi-site deployments.
* Troubleshooted and configured routing protocols including **EIGRP (IPv4/IPv6), OSPFv2/v3, and static routes**; reduced convergence times by **30%** and sustained **99.9% uptime** across campus WAN links.
* Implemented **HSRP and VRRP** on gateway routers, ensuring seamless failover and **sub-second convergence** for critical applications.
* Authored detailed routing diagrams, Visio topologies, and SOPs for standard configs; reduced onboarding time for junior staff by **25%**.
* Resolved WAN outages involving **BGP route reflectors on Cisco Nexus 7000**, diagnosing route flaps and dampening issues; restored stable site-to-site connectivity for **150+ remote branches**.
* Deployed and supported **Cisco ASA 5500 Series firewalls** with IPsec and SSL VPNs, securing remote workforce access for **1,000+ users**; reduced unauthorized login attempts by **35%**.
* Enforced NAT, ACLs, and firewall logging on Cisco ASA, implementing policy-based controls that reduced network breaches by **25%** and improved security visibility.
* Configured **AWS Security Groups and NACLs** as well as **Azure Traffic Manager**, providing secure hybrid-cloud access; supported early stages of multi-cloud adoption with **99.95% uptime**.
* Assisted VMware teams in maintaining **vSphere 6.x and NSX**, troubleshooting VXLAN tunnel drops and DFW policy mismatches; contributed to sustaining **99.5% uptime** for virtual workloads.
* Configured **Citrix NetScaler Gateway with MFA**, troubleshooting SSL VPN tunnels and traffic shaping; improved VPN performance by **20%** for remote developers.
* Managed enterprise Wi-Fi using **Cisco and Aruba APs**, resolving coverage gaps in 2.4/5 GHz bands; deployed **802.1X EAP/PEAP authentication**, cutting unauthorized connections by **30%**.
* Utilized **SolarWinds NPM/NCM, NetFlow Analyzer, Wireshark, and Splunk** for proactive monitoring; identified top talkers and resolved bottlenecks, improving application throughput by **15%**.
* Administered **DNS and DHCP** services across BlueCat, Infoblox, and Windows Server; resolved scope exhaustion and recursive lookup issues, maintaining **99.99% uptime** for core services.
* Participated in **rack, stack, and cabling** of Cisco switches, routers, and firewalls, including fiber patching and labeling; accelerated new site deployments by **25%**.
* Assisted in configuring **site-to-site IPsec VPNs** on Cisco ASA, Palo Alto PA-220, and Fortinet FortiGate 100D devices; provided secure partner connectivity with SLA-driven uptime.
* Supported cloud provisioning by helping configure **AWS VPCs, subnets, and route tables**; documented IP allocations and hybrid-cloud diagrams, improving cross-team collaboration.
* Resolved daily tickets in **ServiceNow**, handling VLAN changes, VPN access requests, and P1/P2 escalations under SLA; built early experience in 24x7 operations and on-call rotations.

**EDUCATION**

Master of Science: Information Technology and Management

Eastern Illinois University