

Tejesh Alaparthi

Harrison, New Jersey, United States | tejeshalaparthi57@gmail.com | (848) 248-1001 | [linkedin.com/in/tejesh-a-1126aa374](https://www.linkedin.com/in/tejesh-a-1126aa374)

PROFESSIONAL SUMMARY

Network Security Engineer with about 5 years of experience designing, securing, implementing, and supporting enterprise network infrastructure across on-premises, hybrid cloud, and AWS environments. Extensive hands-on experience with Palo Alto firewalls, Cisco networking, firewall policy management, IDS/IPS, IPSec/SSL VPN, network segmentation, vulnerability remediation, and security incident response. Strong AWS networking background including VPCs, subnets, route tables, Transit Gateway, Security Groups, NACLs, Route 53, Site-to-Site VPN, and hybrid connectivity. Experienced troubleshooting complex Layer 2–7 connectivity and security issues using packet captures, firewall logs, and CLI diagnostics.

EDUCATION

Rutgers, The State University of New Jersey

Master of Science, Information Technology and Analytics, GPA: 3.58/4.0

Aug 2022 - Dec 2023

Mahindra University

Bachelor of Technology, Computer Science, GPA: 3.4/4.0

SKILLS

Network Technologies: Palo Alto Networks, Panorama, PA-1400/3000/5000 Series, PA-VM, Cisco ASA, Cisco Firepower, Fortinet FortiGate, Check Point, Firewall Policy Management, Security Rules, Access Control Lists, NAT/PAT, IDS/IPS, Threat Prevention, Network Segmentation, Security Zones, Vulnerability Remediation, Incident Response, Security Hardening, Least-Privilege Access

Cloud Networking: Cisco Catalyst 9300/9350/9500, Nexus 9K, ASR, ISR, Cisco Meraki MX, LAN/WAN, VLANs, Inter-VLAN Routing, 802.1Q Trunking, Port Channels, STP/RSTP/PVST+, VPC, HSRP, VRRP, Layer 2/3 Troubleshooting

Routing & Secure Connectivity: BGP, OSPF, EIGRP, Static Routing, Policy-Based Routing, Route Redistribution, Route Filtering, IPSec VPN, SSL VPN, GlobalProtect, Site-to-Site VPN, Remote Access VPN, GRE Tunneling, Hybrid Cloud Connectivity

Cloud Platforms: AWS VPC, Public/Private Subnets, Route Tables, Transit Gateway, VPC Peering, Site-to-Site VPN, Direct Connect, Security Groups, NACLs, Route 53, ALB, NLB, AWS Availability Zones, Azure, GCP, Heroku

Automation & Infrastructure: Terraform, Terragrunt, CloudFormation, Ansible, GitHub Actions, Python, Bash, Git-Based Change Control

Microsoft and Core Network Services: Microsoft Network Environments, Windows 10/11, macOS, DNS, DHCP, NTP, SMTP, RADIUS, AAA, Authentication Services, Endpoint Imaging and Provisioning, MDM (Intune), Enterprise Application Connectivity, Hybrid Name Resolution, SSL/TLS Certificates

Monitoring and Security Troubleshooting: Wireshark, tcpdump, traceroute, nmap, SolarWinds NPM/NCM, NetPath, Zabbix, PRTG, ThousandEyes, Grafana, New Relic, SNMP, Syslog, NetFlow, Firewall Traffic Logs, Packet Capture Analysis

Security and Network Operations: Security Incident Response, Vulnerability Remediation, Root Cause Analysis, Change Management, MOPs, Backout Plans, Network Documentation, Runbooks, Security Updates, Firmware Upgrades, Infrastructure Monitoring, Server Patch Management, Backup and Disaster Recovery, ITIL Frameworks, IT Service Lifecycle Management, Incident Management, Problem Management

WORK EXPERIENCE

Network Security Engineer

Jan 2026 - Present

Collectors Universe, Inc

Jersey City, NJ

- Provide **IT support** as an escalation point for production and corporate users across on-prem and cloud (Azure, AWS, Heroku), driving post-incident improvements and root cause fixes.
- Deliver **Level 1/2 support** for employee endpoints including **desktops**, **laptops**, and mobile devices, resolving OS/app access issues, VPN connectivity, and account-dependent network access blocks.
- Own **infrastructure management** for secure hybrid connectivity, coordinating server, network, and security changes across on-premises infrastructure and AWS/Azure to restore service quickly during outages.

- Design and maintain secure LAN, wireless, and **WAN networks** using Cisco Catalyst switching, Cato SASE, VLAN segmentation, access controls, routing, and site-to-site VPNs across distributed locations.
- Led security incident response, containment, and vulnerability remediation for the critical FortiBleed vulnerability affecting internet-facing FortiGate-VM infrastructure, developing a phased remediation runbook and validating fixes through packet captures, firewall logs, and controlled change procedures.
- Administer and support AWS hybrid networking including VPCs, subnets, route tables, Security Groups, NACLs, DNS, secure routing, and cloud migration connectivity while validating network and firewall changes for least-privilege access.
- Standardized endpoint onboarding runbooks for Android enrollment, **Android devices**, and **iOS devices**, improving Day 1 readiness and reducing setup escalations through clearer knowledge materials.
- Support warehouse and office operations by troubleshooting printing and label workflows, including **Zebra printers**, network print queues, and device connectivity tied to **shipping and logistics tools**.
- Implement and monitor network and infrastructure observability using PRTG, Zabbix, Grafana, and New Relic, proactively identifying availability, performance, and security-impacting issues before they affect critical services.

Senior Network Engineer

Jan 2024 - Dec 2025

Dunton Consulting LLC

Brooklyn, NY

- Administered Palo Alto firewalls and perimeter security infrastructure, including security-policy and access-control rule creation, NAT, IDS/IPS, IPSec/SSL VPN, GlobalProtect, security zones, and centralized firewall management through Panorama.
- Delivered front-line user support during outages by triaging tickets, reproducing issues, and resolving workstation and network access problems across Windows and macOS endpoints.
- Maintained enterprise Cisco/Meraki switching, wireless, firewall, WAN, and VPN infrastructure, troubleshooting complex LAN/WAN, internet, routing, DNS, and application connectivity issues across production environments.
- Performed server and network patch coordination for mixed Windows and Linux estates, scheduling maintenance windows, validating prechecks, and documenting post-patch verification to reduce repeat incidents.
- Investigated and remediated network security vulnerabilities and connectivity incidents using Palo Alto traffic/threat logs, Wireshark, tcpdump, traceroute, and nmap while recommending secure configurations based on least-privilege and industry best practices.
- Planned and executed firewall security updates, patches, firmware upgrades, configuration changes, and infrastructure maintenance using formal change-management processes, MOPs, approvals, implementation plans, backout procedures, and post-change validation.
- Automated access and device troubleshooting steps with **PowerShell scripting** and lightweight scripts to speed up log collection, DNS cache resets, and common endpoint remediation actions.
- Administered core network services and monitored infrastructure through DNS, NTP, SMTP, RADIUS, SolarWinds NPM/NCM, NetPath, Zabbix, and ThousandEyes, collaborating with Microsoft, server, application, and infrastructure environments to maintain secure and reliable connectivity.
- Monitored firewall, IDS/IPS, network-device, and application connectivity events to identify abnormal behavior, troubleshoot potential security issues, and coordinate remediation with security, systems, and application teams.

Network Engineer

Feb 2020 - Jul 2022

Accenture

Bangalore, India

- Designed, deployed, and maintained secure enterprise and data-center network environments using Cisco Nexus 9K, Cisco CSP, Palo Alto firewalls, Fortinet firewalls, and Meraki security appliances across multiple colocation locations.
- Configured and supported BGP, VLANs, VXLAN, routing, segmentation, firewall connectivity, and access controls to provide scalable and secure connectivity for customer infrastructure.
- Performed Palo Alto firewall, Fortinet firewall, Nexus switch, and Cisco CSP security/firmware updates, including pre-change validation, documented implementation procedures, rollback planning, and post-change verification.
- Monitored and troubleshoot network security, BGP, routing, packet-flow, and connectivity incidents using NSO, NetFlow, system logs, tcpdump, traceroute, packet captures, and performance analysis in 24x7 environments.
- Automated network service-chain and policy deployments using Python, Bash, JSON, and XML, while maintaining network configurations, change records, technical documentation, and customer deployment procedures.
- Analyzed existing firewall, routing, switching, and security configurations to understand end-to-end traffic flows and implement network changes without disrupting customer production environments.
- Partnered with engineering and customer teams to investigate infrastructure defects, remediate network vulnerabilities, validate software fixes, and maintain secure and reliable customer network environments.

- Designed, implemented, and supported enterprise Cisco LAN/WAN infrastructure using VLANs, OSPF, BGP, HSRP, routing, switching, and Layer 2/3 troubleshooting across production environments.
- Configured and maintained Palo Alto and Cisco Firepower firewalls, including security rules, ACLs, NAT, static routes, BGP, and segmented application access to protect enterprise networks from unauthorized connectivity.
- Deployed Cisco Meraki SD-WAN and Site-to-Site VPN solutions to establish secure connectivity between distributed enterprise locations and remote infrastructure.
- Performed firewall security changes, Cisco ASA upgrades, NAT configurations, and RADIUS-based authentication integrations using documented maintenance, validation, and rollback procedures.
- Supported F5 BIG-IP load balancers, SSL/TLS certificates, network authentication, and enterprise application connectivity while troubleshooting Layer 1–7 issues using Wireshark, tcpdump, traceroute, and network-device diagnostics.
- Monitored and analyzed firewall, routing, switching, VPN, and authentication traffic to identify connectivity and security issues and implement corrective actions across enterprise environments.
- Maintained secure network access through RADIUS, ACLs, firewall policies, network segmentation, SSL certificates, and controlled configuration changes, supporting reliable connectivity between users, servers, and business applications

CERTIFICATIONS & ACHIEVEMENTS

- | | |
|---|----------|
| • CCNP - Cisco Certified Network Professional - Cisco Academy | Jan 2023 |
| • CCNA - Cisco Certified Network Associate - Cisco Academy | May 2020 |
| • CompTIA Network + - CompTIA | Feb 2019 |