Varshini Basavarajappa
Sr. Network Engineer
Varshinisherapurb@gmail.com
312-478-2134

Professional Summary:

- Having 9+ years of experience designing, implementing, and securing large-scale enterprise networks using Cisco ASA 5525-X, Palo Alto PA-5220, and Fortinet FortiGate v7. Specialized in routing, switching, and firewall migrations.
- Hands-on experience with Cisco Nexus v9k, Catalyst 9300 Series, and Juniper EX/MX routers for core and distribution layers. Expert in OSPF v2, BGP v4, and MPLS v3 routing architectures and policy control.
- Proficient in Palo Alto PA-5220, PA-3060, and PA-5000 series firewalls. Managed policies in Layer 3 and vWire modes, integrated with Panorama, Cisco ISE v3.0, and LDAP for identity-based enforcement.
- Designed end-to-end SD-WAN architectures using Cisco Viptela and Silver Peak v9, including TLOC extensions, centralized policies, and cloud breakout for over 100 branch sites.
- Configured Checkpoint R80.30 clusters using ClusterXL for high availability, IPS rule enforcement, and log correlation with external SIEM tools. Led migration from legacy rule bases and optimized policy layers.
- Experienced in AI-driven network operations (AIOps) using Azure Monitor, Azure Sentinel, Splunk, and automation platforms to proactively detect anomalies, predict outages, and optimize hybrid cloud network performance.
- Implemented Zero Trust v3 using Cisco ISE v3.0, Zscaler ZIA/ZPA, and Azure AD. Integrated 802.1X posture assessment and dynamic VLAN tagging across wired and wireless networks.
- Integrated enterprise security operations with Zscaler-aligned monitoring workflows, including log analysis, traffic visibility, incident investigation, and security policy optimization.
- Managed Cisco ASA 5500-X and Firepower Threat Defense (FTD v6.2), applying deep packet inspection, SSL decryption, AMP v5 integration, and URL filtering for perimeter protection.
- Automated provisioning using Ansible v2.9 and Terraform v1.1 across Nexus switches, ASA firewalls, and Juniper SRX650s. Enabled IaC workflows with rollback and version control.
- Configured QoS v6.1 to prioritize VoIP (DSCP 46), video (DSCP 34), and critical banking apps. Applied class-based policies and shaping across WAN links and MPLS interfaces.
- Designed high-density Wi-Fi 6 environments using Cisco WLC v9800 and Aruba 300 Series. Implemented WPA3, ClientMatch, 802.11r, and band steering for optimized performance.
- Integrated Cisco ISE v3.0 with Aruba ClearPass and Infoblox v8.3 for centralized NAC and IPAM automation. Enforced SGT-based segmentation and real-time DNS/DHCP sync.
- Implemented F5 Big-IP v14.1 (LTM/GTM) and Citrix ADC v13 for load balancing. Configured SSL offloading, SNAT, and persistence profiles to support distributed services.
- Assisted with Zscaler SASE architecture initiatives by analyzing user traffic flows, security policies, DNS requests, and application connectivity across hybrid enterprise environments.
- Hands-on experience integrating AI/ML-based analytics with network monitoring, firewall logs, SD-WAN telemetry, and cloud infrastructure to improve incident response and operational efficiency.
- Led wireless deployments using Aruba Virtual Controllers and RFProtect. Performed surveys with Ekahau and Clarity to ensure RF integrity and SLA compliance.
- Generative AI tools and Python-based automation for network troubleshooting, configuration validation, documentation generation, and operational workflow optimization.
- Designed and enforced firewall policies across Fortinet FortiGate v7, Cisco ASA 5525-X, and Checkpoint R80.30 using policy-based NAT and service object hierarchies.
- Built L2/L3 topologies using VLANs (10–80), VTP, HSRP, RSTP, Port-Channels, and routed SVIs. Tuned STP behavior with root guard and BPDU filters for campus-wide stability.
- Configured and monitored AWS VPCs, Direct Connect, Transit Gateway, Route 53, and Security Groups. Supported microsegmentation and service discovery for hybrid cloud.
- Designed GCP environments with firewall rules, IAM roles, SCC policies, and VPN tunnels for production and DR connectivity. Managed compliance and policy inheritance.
- Performed upgrades and clustering for Juniper SRX240, SRX320, and SRX650 firewalls. Applied NAT pools, IDS/IPS, and security zones across distributed environments.
- Integrated Infoblox v8.3 with DNSSEC, IPAM templates, and DHCP scopes. Enabled reverse zone automation and subnet allocation via REST API v3.
- Automated security operations tasks related to Zscaler policy validation, firewall rule audits, configuration checks, and compliance reporting using Python, Ansible, and Terraform.
- Worked on Panorama for centralized Palo Alto firewall rule pushes, template stack configurations, and zone log forwarding to Splunk for visibility.
- Supported voice and video infrastructure including Cisco Telepresence and SIP gateways. Applied QoS and SCCP/H.323 prioritization on WAN routers.

Technical Skills:

Category	Technologies, Skills, and Tools
Cloud Networking	Azure (Virtual WAN, ExpressRoute, VPN Gateway, NSG, Firewall Premium, WAF, Load Balancer, Front Door, API Management, DNS, Sentinel), AWS (Direct Connect, ELB, Shield, Transit Gateway, API Gateway), Hybrid & Multi-cloud Integration
SD-WAN	Cisco Viptela (vEdge/cEdge), Palo Alto Prisma SD-WAN, Fortinet Secure SD-WAN
Firewalls & Security Appliances	Palo Alto (PA-3220, PA-5220), Fortinet FortiGate (100F, 600E), Cisco Firepower (2110, 2130, 4100 Series), Cisco ASA (5500-X), FortiNAC, Panorama, Cortex XSOAR, FortiManager
Zero Trust & NAC	Cisco ISE (3615), FortiNAC, Palo Alto Cortex XDR, ZTNA, Cisco Duo, Okta, TrustSec
Routing & switching	BGP, OSPF, MPLS (L3VPN), VXLAN, EVPN, DMVPN, IPsec, SSL VPN, Cisco Catalyst 9000, Nexus 9000, ASR 1000, ISR 4000, Juniper MX/SRX, Arista 7050X
Load Balancing & ADC	F5 Big-IP (LTM, GTM, ASM – iSeries), Citrix NetScaler/ADC (VPX/MPX), Azure Traffic Manager
Automation & IaC	Ansible (Tower/AWX), Terraform (modular/IaC), Python (scripting), Git, Jenkins, GitLab CI/CD
Monitoring & Troubleshooting	Wireshark, TCPdump, NetFlow Analyzer, ThousandEyes, SolarWinds, PRTG, Azure Monitor
DNS, DHCP, IPAM	Infoblox (TE-820), Azure DNS, DHCP Failover
Wireless Networking	Cisco Meraki (MR56), Aruba (AP-515), RF Tuning, Site Surveys (Ekahau/ NetSpot), 802.1X Authentication
Application & API Security	Azure WAF, FortiWeb, F5 ASM, Cloudflare, Akamai Kona/Ion, Azure API Management, AWS API Gateway
SIEM & Threat Detection	Splunk Enterprise Security, IBM QRadar, Azure Sentinel
Disaster Recovery & HA	Azure Availability Zones, F5 GTM, SD-WAN Failover, Multi-region DR, ExpressRoute Redundancy
Kubernetes Networking	AKS, Calico CNI, Istio Service Mesh, NSX-T, Microsegmentation, TLS Ingress
QoS & Performance	QoS (CBWFQ, LLQ, WRED), Traffic Shaping, Bandwidth Reservation
Compliance & Governance	HIPAA, HITECH, HITRUST, PCI-DSS, ISO 27001, NIST 800-53, FFIEC, GDPR
DDoS Protection	Cloudflare Magic Transit, Azure DDoS Protection, Arbor Networks (APS, TMS), Akamai Prolexic
DevSecOps Integration	Terraform Cloud, GitOps, Security in CI/CD Pipelines, API Security Policies
Collaboration & Leadership	Team Mentorship, Cross-Functional Collaboration, Architecture Reviews, SOP Documentation, Technical Leadership

Professional Experience:

Grant Thronton, Aurora IL **Mar 2025 – Till Date**
Sr. Network Engineer

Responsibilities:

- Designed and managed enterprise firewalls using Palo Alto PA-7000/5000/3000 series. Enabled App-ID, Threat-ID, User-ID, and HA clustering for secure segmentation.
- Deployed Fortinet FortiGate v7 at remote clinics for firewalling, site-to-site VPN IPSec v3 (RFC 6071), and SD-WAN policy routing. Tuned FortiOS IPS and UTM features.
- Migrated VPN and security policies from Cisco ASA 5525-X to Firepower FTD v6.2. Configured AMP v5, ACP policies, and real-time malware prevention via FMC.
- Deployed Check Point R80.30 ClusterXL across data centers. Managed SmartConsole rulesets, IPS profiles, and SmartView logging with Splunk export.
- Installed Cisco Viptela SD-WAN with vSmart/vEdge/vBond at 200+ branches. Enabled DIA breakout, TLOC extensions, and SaaS acceleration.
- Managed Citrix ADC v13 for load balancing, VPN, and global access control. Enabled SSL offloading, session persistence, and HA pairs.
- Utilized AI-powered monitoring and analytics solutions to detect traffic irregularities, forecast WAN congestion trends, and improve SD-WAN path optimization across multi-cloud environments.
- Integrated Cisco ISE v3.0 with switches and wireless for SGT, 802.1X, and posture-based dynamic VLAN assignment.

- Used F5 BIG-IP v14.1 (LTM/GTM) for application load balancing and failover. Configured SNAT, persistence, iRules, and DNS-based GSLB.
- Supported Zscaler Zero Trust / SASE security initiatives by implementing secure access controls, cloud security policies, traffic inspection workflows, and segmentation strategies across hybrid enterprise environments.
- Deployed SD-WAN overlays using Silver Peak v9 in branch mergers. Applied WAN optimization, BFD monitoring, and route convergence tuning.
- Maintained Infoblox v8.3 for DNS, DHCP, and IPAM. Integrated with Terraform and Python via REST API v3 to auto-update zones and records.
- Wrote Ansible v2.9 playbooks to automate firewall rules, VLAN provisioning, and ACL deployments across ASA, Fortinet, and SRX platforms.
- Managed GCP hybrid cloud networking — VPCs, VPNs, Interconnects, firewall rules, IAM, SCC alerts. Enforced Zero Trust v3 across services.
- Developed automated workflows using Python and Terraform to support AI-assisted configuration validation, compliance checks, and day-to-day cloud network operations.
- Used Terraform v1.1 to build and manage GCP infra: Load balancers, IAM roles, VPC peering, and static routes.
- Scripted Python for Infoblox integration, firewall log parsing, and BGP monitoring automation. Triggered Slack alerts via REST API v3.
- Enabled IPv6 dual stack across internal labs. Assigned 2001:db8::/64 subnets, implemented OSPFv3, and validated address resolution.
- Used SolarWinds v2023 and Wireshark v4.0 to monitor latency, interface drops, and routing convergence. Tuned NetFlow exports and SNMPv3.
- Hardened Cisco ASA 5525-X firewalls with advanced NAT, SSL decryption, and IPS signatures. Enabled high availability and path failover.
- Tuned F5 BIG-IP v14.1 health monitors and fallback pools for resilient service delivery. Applied SSL profile tuning for backend servers.
- Configured Citrix ADC v13 with VPN tunneling, TCP optimizations, and ACL segmentation. Deployed gateway policies for external contractors.
- Enforced policy clean-up across Fortinet FortiGate v7, Checkpoint R80.30, ASA 5525-X. Removed redundant rules and optimized object reuse.
- Deployed Ansible v2.9 tasks via Tower to audit ACLs, SNMP configs, and version compliance for all network nodes.
- Performed IPv6 DNS failover testing using Infoblox v8.3. Built reverse lookup zones, AAAA records, and tested recursive resolution paths.
- Monitored data plane traffic using Wireshark v4.0, TCPdump, and SPAN sessions. Validated IPSec tunnel health and BGP session uptime.
- Built Terraform v1.1 modules for re-usable SD-WAN, Fortinet firewall, and VLAN configuration across dev and prod networks.
- Mentored teams on API Integration v3 use cases for firewall automation, DNS record control, and Slack/Splunk alert integrations.
- Maintained Juniper MX480 and SRX650s for MPLS Layer 3 VPNs, BGP v4, OSPF v2, and EVPN overlays with Netconf and PyEZ automation.
- Applied QoS v6.1 policies for voice/video DSCP 46/34, queue tuning, and policing on WAN interfaces of Cisco ASR 1001-X and Nexus v9k.
- Reviewed and tuned IPSec v3 Phase 1/2 timers, proposals, and crypto ACLs across FortiGate, ASA, and SRX firewalls.
- Documented Visio diagrams, topology maps, and object groupings across ASA, Checkpoint, Fortinet, and Palo Alto platforms.
- Conducted BGP v4 policy audits. Used route-maps, MED, AS-path prepending, and prefix-lists to influence outbound traffic.

Environment: Palo Alto PA-7000/5000/3000, Cisco ASA 5525-X, Firepower FTD v6.2, Fortinet FortiGate v7, Checkpoint R80.30, Cisco ISE v3.0, Cisco Viptela SD-WAN, Silver Peak v9, Citrix ADC v13, F5 BIG-IP v14.1, Cisco ASR 1001-X, Catalyst 9300, Nexus v9k/7k, Juniper SRX650/240/320, MX480, Aruba, Meraki

Capital One, Redmond, VA **Nov 2023 - Feb 2025**
Senior Network Engineer

Responsibilities
- Engineered enterprise network security architecture using Checkpoint R80.30, Fortinet FortiGate v7, and Cisco ASA 5525-X, optimizing segmentation and traffic filtering.
- Deployed BGP v4 (RFC 4271), OSPF v2 (RFC 2328), and MPLS v3 routing protocols to support multihomed WAN infrastructure across 35+ sites.

- Designed and implemented HA firewalls using Palo Alto PA-5220, Checkpoint R80.30, and Fortinet FortiGate v7, with IPSec v3 tunnels (RFC 6071, Protocols 50/51) for secure site connectivity.
- Configured SD-WAN (Viptela v9 and Silver Peak v9) with dynamic path selection and QoS v6.1 for VoIP and cloud SaaS applications.
- Supported Zscaler ZPA-style Zero Trust access models by enforcing least-privilege access, network segmentation, secure remote connectivity, and identity-based security policies.
- Managed Cisco ISE v3.0 for 802.1X authentication, posture assessment, and MAC-based bypass policies across VLANs 20–60 with IP ranges 10.10.10.0/24 to 10.10.60.0/24.
- Integrated Zero Trust v3 principles by segmenting east-west traffic using Cisco ASA, Palo Alto PA-5220, and Fortinet FortiGate v7.
- Automated firewall compliance checks, ACL validation, and rule cleanup using Python, Ansible v2.9, and Terraform v1.1 across 180+ firewalls.
- Streamlined API Integration v3 with Infoblox v8.3 for dynamic DNS updates and automated DHCP reservations.
- Worked with Azure Monitor, Splunk, and network telemetry tools to proactively identify performance issues, firewall anomalies, and routing problems across hybrid cloud environments using AI-driven monitoring and analytics.
- Monitored network health and device uptime using SolarWinds v2023, Wireshark v4.0, and NetFlow Analyzer with SNMP v3 traps.
- Configured F5 BIG-IP v14.1 and Citrix ADC v13 appliances for application delivery, SSL offload, and global server load balancing.
- Performed dual-stack deployments of IPv4 and IPv6 (2001:db8::/64) with DHCPv6, SLAAC, and OSPFv3 routing across core routers and switches.
- Deployed access and trunk port configurations across VLANs 100–199 and interfaces Gi1/0/1 to Gi1/0/48 using Cisco Catalyst 9500s.
- Hardened perimeter devices including Juniper SRX, Cisco ASA, and Fortinet FortiGate v7 with DoS profiles, logging, and secure SNMP/SSH access.
- Used Generative AI and automation tools to support network troubleshooting, configuration reviews, and technical documentation, helping reduce manual effort and improve response times during incidents.
- Created and maintained Terraform v1.1 templates for provisioning cloud firewall rules and dynamic routing gateways in AWS and Azure.
- Enforced segmentation rules across SD-WAN, firewalls, and NAC using Zero Trust v3 framework, ensuring micro-perimeter enforcement.
- Managed SSL certificate lifecycles and WAF policies on F5 BIG-IP v14.1 and Citrix ADC v13 for internal and public web applications.
- Integrated AIOps practices with Python scripting and REST APIs to automate event correlation, streamline remediation tasks, and improve operational visibility across Azure and AWS platforms.
- Enabled full visibility for SOC teams by forwarding syslog and NetFlow data from Checkpoint, Palo Alto, and Cisco ASA to Splunk and SIEM tools.
- Configured NAT/PAT, access rules, and threat profiles across Fortinet FortiGate v7, Checkpoint R80.30, and Palo Alto PA-5220.
- Wrote Python scripts for parsing firewall logs, extracting interface counters, and validating route redistribution scenarios.
- Tuned QoS v6.1 policies and shaping mechanisms across SD-WAN, WAN routers, and voice VLANs 150–159 for unified communications.
- Deployed GSLB using Citrix ADC v13 and GTM features on F5 BIG-IP v14.1 for application failover and geographic load distribution.
- Validated IPv6 (2001:db8::/64) and IPSec v3 configurations with ping, traceroute, and phase-2 tunnel inspection utilities.
- Collaborated on Azure routing design with ExpressRoute and UDRs; validated connectivity between subnets 10.20.0.0/16 and on-prem networks.
- Tuned DNS zones, DHCP scopes, and IPAM policies in Infoblox v8.3 to eliminate conflicts and enforce naming conventions.
- Led firewall upgrades and hotfix rollouts across Checkpoint R80.30 clusters, Cisco ASA 5525-X pairs, and Fortinet FortiGate v7 nodes.
- Standardized tagging, routing, and security rules for AWS EC2, VPC, and Transit Gateway configurations using Terraform v1.1 modules.
- Analyzed application slowness and packet drops using Wireshark v4.0 and SolarWinds v2023 NPM dashboards; resolved MTU and duplex mismatches.
- Hardened VPN access policies and split-tunneling options across Fortinet FortiGate v7, Checkpoint R80.30, and Palo Alto PA-5220.

- Maintained audit-ready documentation for every VLAN ID, IP subnet, interface number, firewall rule, and NAT statement across all zones.
- Assisted DR team in simulating site failovers and restoring BGP v4 and MPLS v3 routing under Zero Trust v3 enforcement layers.
- Maintained and updated Agile story cards and incident tickets in Jira, ensuring accurate documentation of work progress, troubleshooting steps, and resolution details across network change management workflows.
- Designed and deployed cellular backup solutions using LTE/5G failover for critical branch sites, ensuring continuous WAN connectivity during primary link outages and supporting overall SD-WAN resilience strategy.
- Conducted capacity planning and performance tuning exercises across WAN and data center fabrics, leveraging NetFlow analytics and SolarWinds dashboards to forecast bandwidth growth and support business scalability.
- Applied DevOps practices and CI/CD pipeline integration using Jenkins and GitLab CI to automate network configuration validation, testing, and deployment across multi-vendor environments including Cisco, Juniper, and Palo Alto platforms.
- Led network upgrade and migration projects across data center fabric infrastructure using MP-BGP EVPN and VXLAN overlays on Cisco Nexus 9000 platforms, ensuring minimal disruption through phased rollout and rollback planning.
- Developed and maintained network standard operating procedures (SOPs) and templates for firewall policy management, VLAN provisioning, SD-WAN onboarding, and incident response, streamlining operations across junior and senior engineering teams.
- Responded to network incidents and outages with structured resolution strategies; led root cause analysis for BGP, IPSec, and SD-WAN failures across 35+ enterprise sites, reducing mean time to resolution through automation-assisted diagnostics.
- Led Hypernet to Hyperscaler infrastructure migration for Cigna's enterprise network, transitioning on-premises Hypernet fabric to Azure and AWS hyperscaler platforms; redesigned routing, segmentation, and connectivity architecture to align with cloud-native networking standards.

Environment: Cisco ASA, Fortinet FortiGate, Checkpoint, Palo Alto, Juniper, Cisco ISE, F5 BIG-IP, Citrix ADC, SD-WAN, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, IPv6, Zero Trust, API Integration, BGP, OSPF, MPLS, IPSec, AWS, Azure

Humana, Louisville, KY **Oct 2021 - July 2023**
Sr. Network Engineer

Responsibilities:
- Deployed Fortinet FortiGate v7 firewalls across VLANs 101–106 with TCP/UDP port-based ACLs, NAT/PAT, and application-layer filtering. Used interface port1–port3 for segmented enforcement. Integrated firewall clusters into Zero Trust v3 zones.
- Built IPSec v3 tunnels (RFC 6071) to Azure over UDP port 4500 using IKEv2, Protocol 50 (ESP), and fallback detection timers. Applied Phase 1 DH Group 21 and Phase 2 selectors for 10.10.10.0/24 networks.
- Supported Zscaler SASE architecture initiatives by enhancing secure cloud access, internet traffic protection, and policy-driven security enforcement across distributed enterprise environments.
- Configured Palo Alto PA-5220 firewalls with App-ID, User-ID, and SSL decryption rules for internal and DMZ zones. Managed traffic policies over interfaces Ethernet1/1–1/4 with URL filtering for TCP 443 and 8443.
- Maintained Juniper EX switches with BPDU Guard, port security, storm control, and VLAN tagging on ge-0/0/5 to ge-0/0/20. Integrated with RADIUS via Cisco ISE v3.0 for dynamic VLAN enforcement.
- Built SD-WAN overlays using Silver Peak v9 with dynamic path selection, SLA-based routing, and jitter buffering. Enabled packet duplication for VoIP VLAN 120 using QoS v6.1.
- Automated security operations tasks supporting Zscaler and firewall security workflows using Python, Ansible, and Terraform for policy validation, configuration management, and compliance improvements.
- Integrated Cisco ISE v3.0 with 802.1X and MAC Authentication Bypass (MAB) to control wired access. Used TCP 1812 and dynamic ACLs to restrict lateral movement under Zero Trust v3.
- Authored Ansible v2.9 playbooks to push NAT, ACL, and object-group changes across Cisco ASA 5525-X. Vault-encrypted credentials were rotated monthly using CI/CD workflows.
- Deployed Terraform v1.1 modules to provision Checkpoint R80.30 and Citrix ADC v13 in AWS and GCP. Integrated static and dynamic routes with platform-native routing tables.
- Enabled BGP v4 (RFC 4271) for WAN failover with AS prepending and community tagging. Used route-maps to manipulate outbound announcements on interfaces Gi0/2–Gi0/4.
- Engineered OSPF v2 (RFC 2328) area design with virtual links and passive interface configs. Applied MD5 authentication for secure adjacencies on VLAN 105.
- Configured Citrix ADC v13 with SSL offloading, L7 traffic steering, and HTTP header rewrites. Managed services on ports 443, 8443 with integrated health monitors.

- Managed F5 BIG-IP v14.1 with iRules, SSL profiles, and advanced load balancing for HTTPS apps. Used LTM stats and SNMPv3 polling for telemetry via SolarWinds v2023.
- Created IPv6 dual-stack routing (2001:db8::/64) with stateless DHCPv6 and RA. Validated path MTU, DNS resolution, and segment reachability through Infoblox v8.3.
- Tuned SolarWinds v2023 alerts for BGP down events, IPSec tunnel failures, CPU over-utilization, and memory thresholds. Forwarded events via API Integration v3.
- Captured traffic using Wireshark v4.0 to analyze VLAN 106 packet loss, retransmissions, and TCP handshake failures. Isolated congestion on interface Gi0/3 queue.
- Automated DNS and DHCP provisioning through Infoblox v8.3 REST API Integration v3. Handled forward/reverse zones for 10.20.0.0/16 and 10.30.0.0/16.
- Hardened Checkpoint R80.30 using SmartDashboard; applied Application Control and Threat Prevention profiles with user-based rule mapping for RDP/SSH.
- Built IPv6 BGP v4 (RFC 4271) adjacencies to cloud edges. Implemented route filtering with prefix-lists and validated propagation using traceroute6 from VLAN 104.
- Maintained Cisco ASA 5525-X HA failover configurations and monitored sync status on ports Gi0/0–Gi0/1. Audited object groups and NAT rules monthly.
- Created Python utilities for daily firewall audits across Juniper, ASA, and Palo Alto. Used API Integration v3 to extract rules, interfaces, and hit counts in JSON.
- Managed SD-WAN orchestration via Viptela v9; optimized routing paths with jitter thresholds and path-loss metrics. Enforced dual-homing with cloud-edge handoff.
- Built custom dashboards in SolarWinds v2023 to monitor CPU, memory, tunnel status, and packet flows on IPSec v3 links. Tuned alerts to reflect SLA violations.
- Applied Zero Trust v3 policies using Cisco ISE v3.0 tagging and port-based segmentation. Restricted inter-VLAN access via dynamic ACLs and policy bindings.
- Provisioned Terraform v1.1 code for GCP route tables, security groups, and DNS records. Integrated validations into GitLab CI/CD for drift detection.
- Used Wireshark v4.0 to capture DSCP-tagged VoIP packets on VLAN 120 and traced loss patterns. Verified QoS v6.1 prioritization using class-based shaping profiles.

Environment: Fortinet, Cisco ASA, Checkpoint, Palo Alto, Cisco ISE, Juniper, F5 BIG-IP, Citrix ADC, SD-WAN (Silver Peak/Viptela), SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, IPv6, BGP, OSPF, IPSec, AWS, Azure, GCP

Johnson & Johnson, NJ **July 2019 - Sep 2021**
Network Engineer

Responsibilities:
- Deployed Cisco Catalyst 9300 and Juniper EX4600 for high-density studio switching, applying VLAN IDs 10, 20, 100 over interfaces Gi0/1 to Gi0/48 and xe-0/0/1 to xe-0/0/4.
- Configured Checkpoint R80.30, Cisco ASA 5525-X, and Fortinet FortiGate v7 firewalls to enforce NAT, VPN, and Zero Trust v3 across 172.16.0.0/12 and 10.0.10.0/24 zones.
- Deployed Palo Alto PA-5220 with app-based rules, SSL inspection, and wildfire filtering for securing content editing and delivery applications.
- Integrated Cisco ISE v3.0 for dynamic VLAN assignment, 802.1X authentication, and posture checks in guest and studio subnets.
- Engineered SD-WAN using Silver Peak v9 and Viptela to interconnect studios, with QoS v6.1 and DIA breakout for high-definition video traffic.
- Automated provisioning using Ansible v2.9 and Terraform v1.1 for VLAN creation, ACL binding, and switch configuration across Juniper and Cisco devices.
- Created Python scripts to back up firewall configurations, validate BGP neighbor states, and update Citrix ADC v13 GSLB entries via API Integration v3.
- Monitored studio traffic using Wireshark v4.0 and SolarWinds v2023, capturing UDP 5004, 5060, and 16384 during live feed broadcasts.
- Configured F5 BIG-IP v14.1 LTM and GTM for TLS offload, session persistence, and app-layer security on TCP 443 and UDP 53.
- Built Citrix ADC v13 content switching and load balancing policies to optimize traffic distribution for web-based studio tools.
- Tuned routing protocols: BGP v4 (RFC 4271), OSPF v2 (RFC 2328), and EIGRP on Cisco and Juniper SRX routers for dynamic path optimization.
- Applied firewall hardening techniques across Checkpoint R80.30, ASA 5525-X, and FortiGate v7 by enforcing CoPP and locking down management ports.

- Implemented IPv6 (2001:db8::/64) in production and guest zones, enabling NAT64 and DNS64 for dual-stack accessibility and compliance.
- Configured IPSec VPNs using RFC 6071 protocols on Fortinet FortiGate v7, ASA 5525-X, and PA-5220 for secure branch-to-core media sync.
- Tuned QoS v6.1 to prioritize VoIP, video rendering, and real-time collaboration tools on VLANs 120 and 160 using CBWFQ.
- Used API Integration v3 with Terraform v1.1 and Python to dynamically apply route-map changes and firewall rule updates in GCP and AWS.
- Managed DHCP/DNS using Infoblox v8.3, automating AAAA/A records and IPAM tracking across multiple content networks.
- Deployed Zero Trust v3 architecture using Cisco ISE v3.0 profiling and Palo Alto PA-5220 zone-based isolation for external users.
- Enabled SNMPv3 and NetFlow v9 telemetry via SolarWinds v2023, sending syslogs to Splunk and FortiSIEM for studio-wide alerting.
- Created automated rollbacks in Ansible v2.9 for firewall objects and NAT translations across Checkpoint, ASA, and Fortinet appliances.
- Hardened studio endpoints and firewall perimeters by disabling unused protocols (TCP 23, UDP 69) and applying logging standards.
- Used Wireshark v4.0 to analyze audio/video jitter, broadcast packet drops, and frame loss across interfaces Eth1/1–Eth1/4.
- Deployed and tested disaster recovery failovers across GCP, AWS, and on-prem segments, validating IPSec rekeying intervals and BGP reconvergence.
- Configured Citrix ADC v13 and F5 BIG-IP v14.1 for L7 protection, iRules, and multi-region GSLB across public-facing production portals.
- Collaborated with cross-functional teams to migrate legacy ASA clusters to FortiGate v7 and implement Zero Trust v3 across VLANs 50–90.

Environment: Cisco, Juniper, Palo Alto, Fortinet, Checkpoint, Cisco ISE, F5 BIG-IP, Citrix ADC, SD-WAN, SolarWinds, Wireshark, Splunk, FortiSIEM, Infoblox, Ansible, Terraform, Python, API Integration, VLANs, IPv6, BGP, OSPF, EIGRP, IPSec, QoS, Zero Trust, DHCP, DNS, NAC, VPN, Compliance, Azure, AWS, GCP.

Birlasoft, India **Sep 17 – Jun 2019**
Network Engineer

Responsibilities
- Administered firewall policies across Fortinet FortiGate, Cisco ASA 5525-X, and Checkpoint R80.30 to enforce Zero Trust v3 rules for production and QA zones.
- Implemented BGP v4 (RFC 4271), OSPF v2 (RFC 2328), and MPLS v3 across global delivery sites with automatic route failover and policy control.
- Integrated Palo Alto PA-5220 with Panorama for centralized rulebase control, URL filtering, and IPS protections across VLANs 30–120.
- Used SD-WAN (Silver Peak v9 and Viptela v9) to enable intelligent path selection for apps accessing AWS and Azure platforms.
- Configured and managed Cisco ISE v3.0 for dynamic VLAN assignments using 802.1X with fallback MAB authentication for voice and IoT devices.
- Deployed IPSec v3 tunnels (RFC 6071, Protocol 50/51) between client data centers using Fortinet FortiGate, Checkpoint, and Palo Alto firewalls.
- Wrote Python scripts and Ansible v2.9 playbooks to automate ACL generation, object cleanup, and firewall rule audit reports.
- Managed API Integration v3 with Infoblox to handle dynamic DNS updates and IPAM workflows using automation.
- Troubleshot end-user slowness by inspecting flows in Wireshark v4.0 and monitoring metrics via SolarWinds v2023 dashboards.
- Provisioned VLANs (IDs 10, 20, 60, 100) and assigned subnets (10.10.10.0/24 to 10.10.100.0/24) across access and distribution switches.
- Enabled SSL offloading, session persistence, and traffic redirection using F5 BIG-IP and Citrix ADC in DMZ zones.
- Tuned QoS v6.1 on voice VLAN 150 and video VLAN 160 to prioritize unified communications across the MPLS backbone.
- Enforced Zero Trust v3 segmentation policies on firewalls, NAC, and SD-WAN platforms to isolate sensitive business units.
- Documented IP ranges, firewall rule changes, VLAN IDs, and interface usage (Gi0/1–Gi0/24) for compliance readiness.

- Assisted with Azure Virtual Network peering and security group deployments using Terraform v1.1 modules.
- Applied static NAT, PAT, and dual NAT configurations on Cisco ASA and Fortinet firewalls for external service exposure.
- Monitored SNMP traps and NetFlow records from firewalls and routers using SolarWinds v2023 and correlated alerts with syslogs.
- Configured IPv6 (2001:db8::/64) addressing and routing across LAN/WAN boundaries using OSPFv3 and static fallback.
- Coordinated upgrades and policy pushes on Checkpoint R80.30 gateways, Fortinet FortiGate appliances, and Palo Alto firewalls.
- Participated in DR tests by simulating WAN link failures and observing routing convergence across BGP and MPLS paths.
- Supported Azure Virtual Network peering, private endpoint provisioning, and NAT gateway setup for client delivery sites; configured DNS zones and security group policies on the Microsoft Azure stack to enable secure internal communications and enforce firewall rules across segmented network boundaries.

Environment: Cisco ASA, Fortinet FortiGate, Checkpoint, Palo Alto, Juniper, Cisco ISE, F5 BIG-IP, Citrix ADC, SD-WAN, SolarWinds, Wireshark, Infoblox, Ansible, Terraform, Python, IPv6, Zero Trust, API Integration, BGP, OSPF, MPLS, IPSec, Azure, AWS

Qolsys Softwares, India **Sep 2016 – Aug 2017**
Network Engineer

Responsibilities:
- Configured routing protocols including OSPF, BGP, and EIGRP on Cisco and Juniper routers for enterprise WAN and inter-site connectivity.
- Deployed VLAN segmentation and inter-VLAN routing on Cisco Catalyst 2960/3750 switches with STP, RSTP, and EtherChannel configurations.
- Managed Cisco ASA 5500 series firewalls with ACL, NAT, and IPSec VPN for client network perimeter security.
- Supported wireless network deployments with Cisco WLC, configuring SSIDs, VLAN mappings, and 802.1X authentication policies.
- Used SolarWinds and Cisco Works LMS for network monitoring, SNMP alert management, and availability reporting.
- Assisted in MPLS VPN provisioning and BGP PE-CE peering configuration for enterprise WAN services.
- Performed routine network maintenance including firmware upgrades, configuration backups, and hardware replacement tasks.
- Supported troubleshooting of network incidents including L2 loop events, BGP route withdrawal, and DHCP scope exhaustion.
- Documented network configurations, standard operating procedures, and change management records.

Environment: Cisco ISR 2800/3900, Cisco Catalyst 2960/3750, Cisco ASA 5500, Cisco WLC, Juniper EX Series, OSPF, BGP, EIGRP, MPLS, VLAN, STP, VPN, RADIUS, SolarWinds, Cisco Works LMS.

Technical Enhancements & Projects
- Designed and deployed SD-WAN solutions to optimize branch connectivity and reduce MPLS dependency.
- Implemented network automation using Ansible and Python to streamline configuration management.
- Integrated cloud networking components in AWS and Azure, enabling hybrid cloud environments.
- Configured and managed Palo Alto firewalls including policy creation, NAT rules, and Panorama integration.
- Administered load balancers such as F5 and NGINX for application delivery and traffic optimization.