

Vasanthi Chavali

Senior Network Security Engineer | vasanthic2000@gmail.com | +1 720 745 5343

PROFESSIONAL SUMMARY

Senior Network Security Engineer with 5+ years of experience designing, deploying, and securing enterprise and data center networks on Palo Alto, Fortinet, Cisco, and Check Point platforms. Deep hands-on expertise in next-generation firewalls, network segmentation and microsegmentation, Zero Trust architecture, VPN and SD-WAN, and network access control with Cisco ISE and Aruba ClearPass. Experienced in troubleshooting and resolving network security issues by analyzing FortiGate 6500F, 4800F, and 3200F firewall logs and utilizing diagnostic tools. Managed Palo Alto PA-7050, PA-5450, and PA-3260 firewall software updates and patches through the dashboard, ensuring the devices were running the latest security enhancements. Proven in security operations including SIEM platforms (Splunk, Google SecOps), incident response, root-cause analysis, and vulnerability assessment. Strong automation practice with Python, Ansible, and Terraform, significantly reducing manual effort across firewall operations and compliance auditing. Experienced across AWS and Azure cloud network security, including VPC design, security groups, WAF deployment, and hybrid connectivity. Skilled in F5 load balancing, FortiWeb WAF, and IDS/IPS tuning for layered defense. Delivers compliance-aligned environments across NIST, CIS, PCI-DSS, SOC 2, and ISO 27001 frameworks with disciplined change control. Strong foundation in routing and switching (BGP, OSPF, MPLS), VXLAN EVPN data center fabrics, and networking protocols with applied QoS policy design.

TECHNICAL SKILLS

Firewalls / NGFW: Palo Alto Networks PA-Series (PA-7080, PA-7050, PA-5450, PA-5430, PA-5410, PA-5280, PA-5260, PA-5250, PA-5220, PA-3430, PA-3260, PA-3220, PA-1420, PA-850, PA-445; PAN-OS, App-ID, Threat Prevention, URL Filtering, WildFire, GlobalProtect, vsys), Fortinet FortiGate (6500F, 6300F, 4800F, 3200F, 1800F, 500E, 200E, 100E) with FortiManager / FortiAnalyzer, Cisco ASA (5506-X, 5508-X) / Firepower (4112, 4115, 4125, 4145) / FTD / Secure Firewall (3105, 4215), Check Point, Juniper SRX (4200, 2300), Cisco Meraki MX

Network Security: IDS/IPS tuning, network segmentation & microsegmentation, Zero Trust Architecture (ZTA), ZTNA / SASE (Zscaler ZIA/ZPA), IPsec / SSL VPN, GRE, SD-WAN (Cisco Viptela, Silver Peak), NAT/PAT, ACLs

Network Access Control: Cisco ISE, Aruba ClearPass, 802.1X, RADIUS, TACACS+, FreeRADIUS

SIEM & Security Operations: Splunk, Google SecOps (Chronicle), FortiAnalyzer, incident response, root-cause analysis, threat hunting, log correlation, vulnerability assessment, packet analysis (Wireshark)

Cloud Network Security: AWS (VPC, Security Groups, WAF, CloudFront, CloudWatch, CloudTrail), Azure (NSG, Application Gateway, Front Door, Traffic Manager), hybrid cloud connectivity

Load Balancing / WAF: F5 BIG-IP (LTM, GTM), FortiWeb WAF (OWASP Top 10, bot mitigation), Citrix NetScaler

Automation & IaC: Python, Ansible / Ansible Automation Platform, Terraform, GitHub Actions, REST APIs, Netmiko, OctoDNS, Infoblox

Identity & Access Management: Active Directory, Group Policy (GPO), Okta / MFA, RBAC, least-privilege access

Compliance & Governance: NIST CSF, CIS Benchmarks, PCI-DSS, SOC 2, ISO 27001, ServiceNow change & incident management

Routing & Switching: BGP, OSPF, EIGRP, MPLS, HSRP / VRRP / GLBP, VLAN, VXLAN EVPN, STP / RSTP / MSTP, QoS, Cisco Nexus (9300, 9500, 7018, 7010, 5600, 5548) / Catalyst / ISR (4461, 4431, 4331) / ASR (1001, 1002, 1006), Juniper MX / EX, Aruba

Platforms & Services: VMware NSX-T, Windows Server, Linux (RHEL/CentOS), DNS / DHCP / IPAM (Infoblox, Windows DNS, PowerDNS), SolarWinds

PROFESSIONAL EXPERIENCE

State of Delaware (DTI) | Telecom Technologist | Oct 2025 – Present

Delaware, DE

- Administer enterprise network-security services across FortiGate NGFWs, VMware NSX-T distributed firewalls, Zscaler (ZIA/ZPA), and DNS infrastructure in a Zero Trust-aligned hybrid cloud environment.
- Design and enforce microsegmentation policies with NSX-T distributed firewall groups, isolating workloads and containing lateral movement across environments.
- Implement firewall-policy, security-group, address-object, and allowlist changes; validate source, destination, ports, routing, and application requirements under formal change control.
- Operate ZTNA secure remote access via Zscaler ZPA and Fortinet VPN; integrate Okta MFA and FreeRADIUS authentication for identity-aware access.
- Strengthened protection against emerging threats by applying hardened baseline configurations and standard operating procedures across Palo Alto firewall models PA-7050, PA-5250, PA-5280, and PA-5220.
- Built IPsec and GRE tunnels on Cisco ASR 1001, 1002, and 1006 series routers, providing secure and efficient encrypted communication between remote locations.
- Deployed and maintained FortiGate remote-access and site-to-site VPNs across locations, ensuring secure IPv4 and IPv6 network connectivity.
- Led technical design sessions and solution reviews with client stakeholders, presenting Juniper and multi-vendor network solutions, and ensuring business and technical alignment.
- Configured security zones and policies on Juniper SRX 4200 and SRX 2300 devices, enforcing zone-based segmentation to block unauthorized access.
- Deployed and upgraded Cisco ISR 4461, 4431, and 4331 series routers, applying hardened configurations to strengthen routing security.
- Hardened Cisco routers by tightening IPv4 and IPv6 ACLs and securing system services, reducing the attack surface across the routing infrastructure.
- Automated device configuration management with Netmiko-based Python scripts, ensuring accurate and consistent configurations across the infrastructure.
- Conducted routine audits of Active Directory user accounts, service accounts, and domain controllers to identify security gaps, stale accounts, and misconfigurations, ensuring compliance with NIST and CIS security benchmarks.
- Responded to live security events using the advanced intrusion prevention system (IPS) on PA-5000 series devices, containing threats in real time.
- Worked with investigative firms to set up, deploy, and fix several Cisco Nexus switches, involving the 7010, 7018, 5548, and 5600 models. Maintained Cisco Nexus environments, performing regular firmware upgrades and configuration backups to ensure network stability and security.
- Built and maintained robust monitoring and alerting systems for load balancers using F5 iHealth, SolarWinds, and other NMS tools, ensuring uptime SLAs of 99.99%.
- Correlate firewall, proxy, DNS, and routing telemetry in Splunk and Google SecOps (Chronicle) to triage connectivity, authentication, and application-layer failures and determine allow/deny/misroute decisions.
- Lead incident handling through ServiceNow: investigate network-security incidents, coordinate across application, server, cloud, routing, and security teams, and drive root-cause analysis to resolution.
- Built Python-based security-log reporting automation (firewall/proxy query construction, SecOps event retrieval, IP/CIDR search, CSV reporting), standardizing repeatable operational requests.
- Developed GitHub Actions and Ansible automation for Windows DNS (A/CNAME/TXT records) and external DNS via OctoDNS, with dry-run validation and pull-request-based change review.
- Created domain allowlist validation tooling (exact and wildcard matching) enforcing consistent proxy policy across managed repositories.

- Migrated network-automation job templates and schedules between Ansible Automation Platform environments, validating projects, inventories, credentials, execution environments, and job results.
- Delivered firewall and routing changes for hybrid connectivity across on-premises, data center, and Azure environments, including Azure-hosted automation runners.
- Hardened proxy and TLS-inspection paths; distinguished network-layer from application-layer failures in software-update and proxy incidents.
- Review firewall and proxy rule bases for overly permissive policies and security gaps as part of change governance, remediating misconfigurations before production deployment.

Comcast | Sr. Network Security Engineer | Apr 2024 - Sep 2025

Philadelphia, PA

- Served as primary escalation point for complex enterprise routing, switching, and firewall issues; led resolution of high-impact outages and client escalations.
- Deployed and managed Palo Alto NGFWs (PA-7050, PA-5450, PA-5430, PA-5410, PA-5280, PA-5260, PA-5250, PA-3260, PA-3220) with App-ID, Threat Prevention/IPS, URL Filtering, and WildFire zero-day protection; tuned IPS policies to cut false positives while sustaining threat coverage.
- Architected network segmentation with Palo Alto virtual systems (vsys), isolating business units and optimizing traffic flow across data centers.
- Installed and configured Cisco Secure Firewalls (3100/4200 series) and Firepower 4100 series (4112/4125/4145), protecting 10,000+ endpoints.
- Deployed FortiGate firewalls (6500F, 4800F, 3200F, 1800F, 500E, 200E) for remote-access and site VPNs with IPv4/IPv6 support, SSL inspection, and production policy fine-tuning; hardened Juniper SRX security zones and policies.
- Managed Palo Alto firewall software updates and content upgrades to keep security policies current, providing clients with up-to-date threat protection and risk guidance.
- Configured and optimized firewall rules and policies on Cisco Meraki MX450, MX250, MX100 series devices, ensuring robust protection against unauthorized access and threats.
- Configured VPNs on FTD 2100 devices to ensure secure communication between remote sites and headquarters.
- Deployed Cisco Viptela SD-WAN with integrated security services including network segmentation, antivirus inspection, and IPS/IDS.
- Integrated Aruba ClearPass with existing SIEM systems, enriching alerts with identity context for faster risk identification and investigation.
- Extended network visibility with Cisco Stealthwatch, complementing Cisco Secure Firewall 3100 series (3120, 3105) threat defenses.
- Served as the technical anchor during critical escalations, troubleshooting routing/switching outages, and driving permanent fixes across Juniper and Cisco environments.
- Administered enterprise DNS across multiple ISPs with the Infoblox platform, improving operational efficiency and enforcing consistent DNS security controls.
- Monitored performance using SolarWinds and Riverbed, correlating QoS metrics with end-user latency.
- Built IPsec/GRE VPNs across Cisco ASR/ISR (4461, 4431, 4331) routers and Nexus platforms for secure site-to-site and remote connectivity; deployed GlobalProtect-style remote-access VPN services.
- Deployed Cisco Nexus data center fabrics (9300, 9500, 7018, 5548) with VXLAN EVPN overlays for network virtualization and segmentation; standardized deployments with configuration templates and firmware lifecycle management.
- Configured F5 BIG-IP LTM/GTM for global load balancing and failover; built monitoring and alerting (iHealth, SolarWinds) sustaining 99.99% uptime SLAs.
- Configured WAF policies inspecting inbound and outbound web traffic, blocking malicious activity in real time.

- Integrated NGFW logs into SIEM platforms; built Python anomaly detection correlating WAF logs with SIEM alerts and automated weekly reporting dashboards.
- Performed vulnerability assessments of network security infrastructure by analyzing firewall logs, traffic patterns, and configurations; drove remediation of identified exposures.
- Enforced identity security: administered Active Directory (GPO, OUs, RBAC), integrated MFA and SIEM/endpoint platforms, and audited accounts against NIST and CIS benchmarks.
- Drove automation with Python, Ansible, Netmiko, and Terraform: standardized Juniper/Cisco configurations, automated QoS deployment across 200+ devices, and cut CDN/WAF configuration time by 60%.
- Mentored junior and offshore engineers on routing protocols, automation, and firewall operations; led client-facing workshops on segmentation, SD-WAN, and technical design reviews.

Yamaha Motor | Sr. Network Security Engineer | Jan 2023 - Mar 2024

Atlanta, GA

- Deployed and managed multi-vendor NGFWs (Palo Alto, Fortinet, Check Point) with Layer-7 application control and threat prevention.
- Operated Palo Alto firewalls (PA-5200/3200/5400 series): App-ID, Threat Prevention, URL Filtering, WildFire, custom vulnerability signatures, and IPv4/IPv6 security policies.
- Centralized Fortinet operations with FortiManager; deployed FortiGate (100E-1800F) with HA clustering, SSL inspection, and perimeter/internal segmentation roles.
- Deployed FortiWeb WAF for public-facing applications (OWASP Top 10 profiles, bot mitigation, L7 DDoS detection); integrated with FortiAnalyzer and SIEM for alerting, correlation, and forensics.
- Implemented Cisco Viptela SD-WAN with application-aware routing, segmentation, and integrated IPS/IDS.
- Deployed Cisco ISE for 802.1X NAC and TrustSec segmentation; integrated Aruba ClearPass with SIEM for risk-based monitoring.
- Supported incident response and forensic investigations through NGFW log analysis, packet captures, and security-event correlation.
- Automated alerting and reporting with Python; administered DNS via Infoblox; designed Juniper EX/MX campus and data center networks (BGP, OSPF, VXLAN).

Accenture | Network Security Engineer | Jan 2021 - Dec 2022

India

- Created and enforced firewall policies on Check Point (R75-R77), Palo Alto (PA-400 series), and Cisco ASA (5510-5580) with IPsec VPNs and ACLs across multi-vendor environments.
- Deployed Blue Coat ProxySG for web filtering, RSA SecurID MFA, Digital Guardian DLP, and Zscaler for endpoint and web security.
- Engineered resilient topologies with BGP, OSPF, EIGRP, MPLS, VLANs, STP, and QoS; led complete network deployments including rack, cabling, and configuration validation.
- Implemented Cisco Viptela and Silver Peak SD-WAN; configured Cisco ACI application segmentation and TrustSec policy-based access control.
- Managed F5 BIG-IP (LTM) and VIPRION architectures and Citrix NetScaler for highly available application delivery.
- Administered Cisco ISE for 802.1X endpoint access control; managed Splunk log analytics; monitored via SolarWinds and Wireshark (SNMP, NetFlow, Syslog).
- Automated infrastructure with Terraform and Ansible; managed DNS/DHCP/IPAM on Infoblox; maintained audit-ready documentation and change-control records.

CERTIFICATIONS

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