

CHRIS CLINE

Network Security Engineer

St. Petersburg, FL | 727.648.9028 | chriscline1985@gmail.com | linkedin.com/in/ccline2

PROFESSIONAL SUMMARY

Network Security Engineer with 10+ years of hands-on experience designing, implementing, and maintaining secure network infrastructures that protect enterprise data, applications, and services. Expert in architecting and deploying security infrastructure including next-generation firewalls (Palo Alto, Cisco Firepower, Checkpoint, FortiGate), VPNs, IDS/IPS, and network segmentation technologies. Proven track record designing secure network topologies including DMZs and Zero-Trust architectures while monitoring threats using SIEM tools (Splunk, Wazuh). Strong experience with network security policy development, vulnerability management, compliance frameworks (NIST, PCI-DSS, HIPAA, NERC-CIP), and cross-team collaboration with IT, cloud, and cybersecurity teams. Skilled at performing root-cause analysis, providing Tier-3 escalation support, and maintaining comprehensive technical documentation.

CORE COMPETENCIES

- **Network Security Architecture:** Next-Gen Firewalls (Palo Alto, Cisco Firepower/FTD, Checkpoint, FortiGate), VPNs (IPSec/SSL), IDS/IPS, NAC (Cisco ISE), Network Segmentation, Zero-Trust Architecture, Micro-Segmentation
- **Firewall & Perimeter Security:** Policy Configuration, Security Profiles, Threat Prevention, URL Filtering, SSL Decryption, VPN Tunnels, Site-to-Site & Remote Access VPNs, Firewall Audits & Optimization
- **Monitoring & Threat Detection:** SIEM Tools (Splunk 5+ years, Wazuh), Security Log Analysis, Anomalous Traffic Detection, Incident Response, Threat Hunting, Root Cause Analysis
- **Vulnerability & Risk Management:** Vulnerability Assessments, Patching Coordination, Remediation Tracking, Security Risk Assessments, Security Testing
- **Policy & Compliance:** Security Policy Development, NIST CSF, CIS Controls, PCI-DSS, HIPAA, NERC-CIP, Change Management, Peer Review Processes
- **Cloud & Automation:** Azure, AWS, Python Scripting, Ansible, Infrastructure as Code, Security Automation
- **Core Networking:** TCP/IP, BGP, OSPF, EIGRP, VLANs, Layer 2/3 Protocols, Routing/Switching, Network Troubleshooting, Packet Analysis

PROFESSIONAL EXPERIENCE

Senior Solutions Engineer

Bedroc / Change Healthcare | Nashville, TN | March 2024 – Present

- Architected and deployed secure network infrastructure with comprehensive segmentation and micro-segmentation policies across 100+ healthcare facilities
- Designed Zero-Trust network zones and security architectures reducing lateral movement risk by 65%
- Implemented security features on enterprise switches, routers, and network infrastructure achieving 99.98% uptime
- Provided Tier-3 escalation support for complex network and security issues, resolving 200+ critical incidents
- Collaborated with network, cloud, and cybersecurity teams on architecture reviews and incident response efforts

- Developed security automation using Ansible reducing deployment time by 87% and ensuring consistent policy enforcement

Network Security Engineer Lead (Part-Time Consultant)

Seven Seas Water Group | Tampa, FL | February 2023 – September 2024

- Architected, deployed, and maintained security infrastructure including firewalls, VPNs, and IDS systems across 25+ critical infrastructure facilities
- Deployed Wazuh SIEM platform monitoring network and security logs for threat detection, improving anomaly identification by 60%
- Performed vulnerability assessments and coordinated remediation efforts reducing critical vulnerabilities by 75%
- Developed and enforced security policies and procedures ensuring regulatory compliance for critical infrastructure operations
- Followed change management and peer review processes maintaining detailed documentation and audit trails
- Maintained comprehensive network documentation including diagrams, configurations, inventories, and security baselines

Senior Network Engineer

HCA Healthcare ITG | Nashville, TN | September 2018 – February 2023

- Designed, deployed, and maintained next-generation firewalls (Palo Alto, Cisco ASA/FTD, Checkpoint) and F5 security solutions across 180+ hospitals
- Configured firewall rule sets, security profiles, threat prevention, URL filtering, and SSL decryption protecting 50+ mission-critical applications
- Maintained site-to-site and remote-access VPNs including IKEv1/v2, IPSec, and SSL supporting 5,000+ users with 99.95% availability
- Monitored network and security logs using Splunk SIEM identifying and investigating security incidents and anomalous traffic
- Participated in root-cause analysis and developed mitigation strategies reducing security incidents by 45% year-over-year
- Coordinated patching cycles with IT and operations teams maintaining 99.8% patch compliance
- Developed security policies and procedures ensuring compliance with PCI-DSS and HIPAA regulatory frameworks
- Supported cloud and hybrid environments integrating on-premises security with Azure infrastructure
- Participated in change management meetings, architecture reviews, and project planning with cross-functional teams

Incident Response Technician (Team Lead)

HCA Healthcare ITG | Nashville, TN | November 2016 – January 2018

- Led incident response team providing Tier-3 support for 500+ network and security incidents monthly
- Identified, investigated, and responded to security incidents using SIEM tools and log analysis
- Developed incident response procedures and mitigation strategies reducing MTTR by 40%

EDUCATION & CERTIFICATIONS

Bachelor of Science, Information Technology | Information Security & Assurance

Western Governors University | Salt Lake City, UT | 2016 – 2019

- Cisco Certified Network Associate (CCNA) - Meets CCNP Enterprise equivalency requirement
- CCNA Security
- CompTIA Linux+
- CompTIA Project+