

**Christine Lamothe christineseminole763@gmail.com**

**Sr. Network Engineer**

**Professional Summary:**

* Senior Network Engineer with 10 years of experience designing and maintaining Cisco-based LAN and WAN infrastructures across multi-site Data Center networks, delivering scalable Network Solutions aligned with business needs.
* Expert in performing Network Assessments, implementing Network Access Control using Cisco ISE, and optimizing routing protocols including EIGRP, OSPF, and BGP for high-performance LAN, WAN, and Data Center connectivity.
* Skilled in migrating legacy Cisco platforms to Catalyst 9K switches, enhancing network performance, and deploying Network Access Control policies across enterprise environments.
* Proficient in configuring and deploying Cisco SD-Access to replace traditional ISE, strengthening Network Access Control and optimizing routing in LAN, WAN, and Data Center networks.
* Experienced in managing multi-vendor infrastructures using Cisco ACI, Juniper, Palo Alto, and Fortinet, integrating security products to protect enterprise endpoints.
* Adept at designing secure cloud and on-premise IT solutions using SD-WAN, MPLS, IPsec, and SSL VPNs, improving inter-office connectivity and ensuring service availability.
* Hands-on experience with virtualization and network segmentation using VMware ESXi, NSX, and Hyper-V, supporting multi-tenant operations and maintaining Network Architecture and Mapping.
* Skilled in deploying and managing wireless networks using Cisco Meraki and Ruckus, performing Network Assessments and delivering Network Access Control for mobile users.
* Strong background in troubleshooting complex LAN, WAN, and Data Center issues, leveraging Network Assessments, Network Access Control, and routing optimization with EIGRP, OSPF, and BGP.
* Experienced in planning and executing Cisco platform upgrades, implementing Network Access Control with ISE, and maintaining accurate Network Mapping and Network Architecture.
* Delivered high-availability solutions through network modeling, redundancy planning, and disaster recovery strategies to ensure continuous operation of critical applications.
* Proficient in IT compliance, access control, and perimeter defense using Cisco ASA, Palo Alto, and FortiGate firewalls, implementing Network Access Control to secure enterprise systems.
* Experienced in translating business requirements into technical outcomes, creating Network Mapping and documentation for improved operational clarity across LAN, WAN, and Data Center networks.
* Dedicated to mentoring junior engineers on Network Architecture, Network Access Control, and Network Mapping best practices to enhance team efficiency.
* Certified professional holding CCNP, CCIE (Routing & Switching), and PCNSE certifications, ensuring secure and optimized Network Solutions across enterprise LAN, WAN, and Data Center environments.

**Technical Skills:**

|  |  |
| --- | --- |
| **Categories** | **Technology/Tools** |
| **Cisco Routers** | Cisco Routers 1600, 1700, 2600, 2800, 3600, 7200, and ASR 1000 series routers |
| **Switching** | VLAN, VTP, STP, PVST+, RPVST+, Inter VLAN routing & Multilayer Switching, Multicast operations, Layer 3 Switches, Ether channels, Transparent Bridging |
| **LAN** | Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, CDDI, Token Ring, ATM LAN Emulation |
| **WAN** | Leased lines 64k - 155Mb (PPP / HDLC), Channelized links (E1/T1/E3/T3), Fiber Optic Circuits, Frame Relay, ISDN, and Load Balancing**.** |
| **Cisco ASA Firewall** | Cisco ASA firewall 5000 series (5585) Checkpoint R75.20, R 76 and R 77 |
| **Big IP F5 Load Balancers** | Big-IP 8800 series; Big-IP 8400 series; Big-IP 6400 series; Big-IP 3400 series; Big-IP 1500 series, Viprion. |
| **Protocols** | BGP, OSPF, EIGRP, RIP, QoS, Spanning Tree, IP multicast, IGMP, PIM, VPN, IPSec Tunnel, HSRP, VRRP |
| **Wireless** | Catalyst 6500 Series/7600 Series Wireless Services Module (WISM), Aruba 3600 Controller, AP 93, AP105(Symbol) Motorola 7000, 5100, 3Com Wireless. |
| **Networking Hardware** | Cisco Switches, Cisco Routers, ASA/Pix/Palo Alto/Fortinet/Juniper firewalls. |
| **Firewalls** | Juniper Net Screen (500/5200), Juniper SRX (650/3600), Pix (525/535), ASA (5520/5550/5580), McAfee Web Gateway, Checkpoint, Palo Alto firewalls. |
| **AAA Architecture** | TACACS+, RADIUS, Cisco ACS. |
| **Load balancer** | Nortel Alteon, F5, Big IP Load balancer |
| **IP Telephony** | IP Telephony utilizing Cisco routers, FXO/FXS/E&M/T1/ISDN/ PRI, Call manager (publisher & subscriber) |
| **Security / Firewalls** | Cisco ASA Firewalls 55XX, IPSEC & SSL VPNs, IPS/IDS, DMZ Setup, CBAC, Cisco NAC, ACL, IOS Firewall features, IOS Setup & Security Features |

**Education Details:**

* Bachelors in Computer Science from University of Miami, FL. 2013
* Masters in Computer Science from Harvard University, MA, 2015

**Certifications Details:**

* Cisco Certified Network Professional
* Palo Alto Networks Certified Network Security Engineer
* Certified Information Systems Security Professional
* SD-WAN Certified Specialist

**Professional Experience:**

**EPAM Systems, Newtown, PA June 2023 to Present**

**Sr. Network Engineer**

**Responsibilities:**

* The enterprise deployment of Cisco ACI Spine-Leaf architecture using Nexus 9336PQ and 93108TC-EX, enabling scalable and policy-driven data center fabric. Integrated L2/L3 out and service graphs to enforce segmentation and control. Ensured multi-tenant isolation, high availability, and dynamic service chaining.
* Automated day-to-day ACI provisioning using REST APIs, XML payloads, and Postman, reducing manual tasks and improving deployment accuracy. Integrated scripts with internal tools to simplify operations. Delivered consistent policy enforcement across diverse workloads and tenants.
* Engineered and implemented 100G DWDM-based Data Center Interconnect (DCI) using OTV, MPLS, and vPC technologies. Designed multicast routing with PIM-SSM and Anycast RP to support high-throughput applications. Achieved seamless failover and low-latency east-west data replication.
* Led data center migration from legacy Catalyst 6500 to Nexus 7K/9K with redesigned core routing and modular topologies. Deployed VDCs and vPC to support logical segmentation and redundancy. Improved network performance, reliability, and scalability across environments.
* Managed the migration of mission-critical applications from Cisco ACE to F5 LTM/GTM platforms. Created VIPs, SSL profiles, and iRules to ensure application-aware traffic handling. Enabled global load balancing with WideIP and DNS-based failover mechanisms.
* Performed end-to-end firewall migrations from Cisco ASA to Palo Alto and Check Point platforms. Designed security zones, NAT policies, VPN tunnels, and access controls. Delivered zero-downtime cutovers by leveraging detailed implementation and rollback strategies.
* Designed and maintained enterprise WAN infrastructure using BGP, MPLS, and DMVPN technologies. Implemented redundancy and route filtering for 100+ branch locations. Ensured optimized routing, secure communication, and SLA-based traffic control.
* Configured and supported multicast routing in enterprise networks using PIM-SSM, MSDP, and RP redundancy models. Onboarded multicast sources for real-time applications. Troubleshot IGMP joins, RP elections, and packet drops with precision.
* Implemented Infoblox DNS, DHCP, and IPAM solutions, replacing legacy systems with high-availability infrastructure. Integrated DHCP failover, IP address management, and DNSSEC features. Enhanced visibility, auditability, and operational efficiency.
* Developed Python scripts to automate device configuration across Palo Alto, Nexus, and F5 platforms. Parsed logs, validated compliance, and reduced manual provisioning. Enabled faster deployment cycles and improved network consistency.
* Designed and enforced firewall policies on Check Point and Palo Alto appliances, including rule base optimization, NAT setup, and antispoofing. Deployed IPsec VPNs and remote access tunnels aligned with security standards. Enhanced perimeter security and policy compliance.
* Monitored critical infrastructure using SolarWinds, SevOne, and Splunk dashboards to identify top talkers, bandwidth bottlenecks, and anomalies. Customized alerts for threshold breaches and proactive remediation. Ensured high network availability and optimal performance.
* Provided Level 3 support for complex network outages involving routing, switching, and security platforms. Conducted root cause analysis with TCPDUMP, FWMonitor, and debug tools. Delivered incident reports with actionable remediation steps.
* Engineered QoS policies for VoIP, video, and low-latency financial applications across WAN and LAN. Applied NBAR-based traffic classification and LLQ shaping. Ensured application performance under congestion and met all SLA targets.
* Configured dynamic routing protocols including BGP, OSPF, and EIGRP across core and edge devices. Managed route redistribution, policy-based routing, and filtering. Ensured fast convergence and robust path resiliency across network domains.
* Multiple data center and branch migrations involving hardware refreshes, ISP transitions, and Layer 3 architecture. Created detailed MOPs and coordinated with cross-functional teams. Delivered seamless cutovers with no business disruption.
* Participated in Change Advisory Board (CAB) meetings, presented high-impact changes, and assessed risks. Prepared rollback strategies and test plans. Ensured alignment with ITIL change control policies and reduced change-related incidents.
* Deployed and managed wireless LAN infrastructure using Cisco WLCs and APs, integrated with Cisco ISE for authentication. Tuned RF parameters for optimal coverage. Ensured secure and high-performance wireless access for enterprise users.
* Implemented secondary ISP links with active-passive and BGP-based failover strategies. Tuned local preference and AS-path policies for traffic engineering. Achieved 99.999% availability for internet and business-critical connectivity.
* Maintained and updated high-level and low-level design documents, network topology diagrams, and device runbooks. Ensured up-to-date documentation for audits, onboarding, and troubleshooting. Streamlined support operations and knowledge transfer.

**Environment**: Experience with Cisco ACI 5.2, Nexus 9000 NX-OS 9.3, Catalyst 9000 IOS-XE 17.6, Meraki 15.44, SD-WAN Viptela vManage 20.7, Palo Alto PAN-OS 10.2, Ansible 2.12, Python 3.9, REST APIs, SolarWinds Orion 2023.2, Splunk 9.0, Wireshark 4.0, Azure ExpressRoute Gateway v2, AWS Site-to-Site VPN, VMware vSphere 8.0, Dell EMC Unity XT OE 5.1, Cisco UCS Manager 4.2, Infoblox NIOS 8.6, Windows Server 2022, and RHEL 9.

**Intone Networks, Okemos, MI Jan 2022 to May 2023**

**Sr. Network Engineer**

**Responsibilities:**

* Designed and maintained enterprise-scale LAN/WAN/WLAN environments using Cisco Nexus 9000, Catalyst 9300, and Meraki infrastructure. Integrated advanced Layer 2/3 protocols with HA techniques to ensure consistent network performance across core and distribution layers.
* Implemented next-generation firewall solutions including Cisco Firepower, ASA, and Palo Alto, applying security policies, threat signatures, and VPN configurations for internal and external protection. Built secure edge architectures that aligned with organizational compliance needs.
* Delivered global SD-WAN deployments using Cisco Viptela and Meraki, enabling cloud-first connectivity with dynamic path selection and centralized policy enforcement. Reduced MPLS dependency while improving uptime and application experience.
* Configured dynamic routing protocols such as BGP, OSPF, and EIGRP across multi-site networks, fine-tuning route maps and redistributions for optimal path selection and failover readiness. Ensured network scalability and routing stability.
* Used Ansible and Python-based automation (Netmiko, NAPALM) to deploy configurations, backups, and updates across hundreds of devices. Streamlined network management tasks and eliminated manual errors through templated scripting.
* Established hybrid connectivity between on-prem data centers and public cloud environments via Azure ExpressRoute, AWS Direct Connect, and site-to-site VPNs. Secured interconnectivity with proper BGP routing and IP segmentation.
* Deployed and supported F5 LTM/GTM load balancers, configuring pools, virtual servers, and custom iRules for application redundancy and performance. Enabled high-availability and global traffic distribution for mission-critical apps.
* Troubleshot Layer 2–7 issues using Wireshark, SolarWinds, and NetFlow tools to identify performance degradation, misconfigurations, and security concerns. Conducted deep-dive packet captures and protocol analysis for RCA.
* Engineered enterprise-grade wireless networks using Cisco 9800 WLC and Wi-Fi 6 access points, applying SSID segmentation, CleanAir, and identity-based access. Delivered seamless wireless roaming and stability in high-density environments.
* Integrated Cisco ISE for 802.1X wired/wireless authentication, endpoint profiling, and dynamic VLAN assignment. Built posture-based access control policies to segregate users, guests, and unmanaged devices.
* Maintained secure remote access infrastructure using Cisco AnyConnect, IPSec, and SSL VPNs. Integrated with Duo MFA for identity validation and adaptive access enforcement for remote employees and partners.
* Used SNMP, NetFlow, and syslog-based monitoring (via SolarWinds, Splunk) to track availability, traffic patterns, and anomalies. Set up custom alerts and dashboards for proactive fault and capacity management.
* Executed firmware upgrades and patching cycles across firewalls, switches, and wireless devices in planned maintenance windows. Followed rollback procedures and post-upgrade validation for service continuity.
* Managed DHCP, DNS, and IP address assignments using Infoblox IPAM for centralized visibility and control. Automated IP provisioning and ensured consistent addressing schemes across data centers and remote offices.
* Segmented data center environments with VRF-lite, VLAN trunking, and inter-VRF routing to separate tenant and application traffic. Implemented secure Layer 3 boundaries and policies for regulated zones.
* Configured virtual switching in VMware vSphere with VDS integration, VLAN tagging, and port group templates. Enabled seamless connectivity between virtual machines and physical switches.
* Maintained detailed network diagrams, configuration archives, and topology documentation in Visio and Git repositories. Ensured up-to-date change tracking and handover readiness for support teams.
* Collaborated with security teams to enforce firewall rules, NAC policies, and zoning required for PCI-DSS, HIPAA, and ISO compliance. Participated in audits, vulnerability assessments, and remediation efforts.
* Provisioned VLANs, ACLs, NAT rules, and interconnects as per infrastructure and application team requirements. Provided network readiness for server rollouts, migrations, and application cutovers.
* Planned for capacity growth, port/channel expansion, and device lifecycle replacements through regular infrastructure reviews. Made hardware and licensing recommendations based on usage and forecasted demand.
* Handled escalations and managed vendor relationships with Cisco, Palo Alto, F5, and ISPs to ensure timely support, hardware replacements, and SLAs. Logged and resolved TAC cases for critical incidents.
* Delivered expert-level technical support and architecture for global enterprise IT infrastructure, optimizing LAN/WAN environments using Ruckus, Cisco Meraki, Riverbed, and NSX while ensuring regulatory compliance (GDPR, CISM) and seamless project-based implementation of secure, scalable design solutions

**Environment:** Ansible 2.9/2.12, Python 3.8/3.10, SolarWinds Orion 2020.2, NetBrain 8.0, Cisco Prime Infrastructure 3.8, Wireshark 3.6, Infoblox NIOS 8.5, Cisco ISE 2.7, F5 BIG-IP LTM 15.1, Palo Alto PAN-OS 10.1.

**Capgemini, Atlanta, GA Sep 2020 to Dec 2021**

**Network Security Engineer**

**Responsibilities:**

* Administered and maintained enterprise LAN/WAN infrastructure and security across 3 data centers, resolving over 500 tier 2 and 3 network/security issues annually, ensuring 99.9% uptime.
* Deployed and configured firewalls including Cisco ASA, Palo Alto PA-5000, and Check Point R81.20, enforcing security policies for 15,000+ endpoints and maintaining perimeter defense with zero major security incidents.
* Performed regular rule base reviews and policy tuning using Tufin Orchestration Suite 22.1 and Splunk 9.1, optimizing firewall performance and achieving 100% compliance with enterprise security standards.
* Configured site-to-site and remote access VPNs using IPsec and SSL protocols on Cisco ASA and Check Point, providing secure connectivity for 2,500+ remote users across 10+ branch offices.
* Managed IPS/IDS solutions including Sourcefire 6.5 and FireEye NX, detecting and preventing over 1,000 potential threats per month, and escalating high-severity incidents to the security operations center (SOC).
* Conducted vulnerability assessments using Nessus 10.3, identifying and remediating 200+ critical vulnerabilities quarterly, reducing attack surface by 35% across enterprise systems.
* Configured and supported Blue Coat ProxySG 10.5 appliances for secure web access, URL filtering, and enforcing department-specific browsing policies for 5,000+ users.
* Managed user authentication and policy enforcement using Cisco ISE 2.7, RADIUS, LDAP, and Microsoft Active Directory 2019 integrations, streamlining secure access for internal staff and contractors.
* Built and maintained security tools including Cisco NAC, Websense 10.5, and Aruba ClearPass 6.9, monitoring over 5,000 endpoints and enforcing compliance across corporate networks.
* Created and managed IPSec VPN tunnels with third-party vendors, ensuring secure communication and compliance with DoD and enterprise security standards for 10+ external partners.
* Worked with multiple teams to capture and analyze traffic using TCPDUMP and Check Point SmartView Tracker, reducing troubleshooting time by 25% for cross-site connectivity issues.
* Configured F5 BIG-IP LTM/GTM 15.1 load balancers with virtual servers, iRules, health monitors, and SNAT, optimizing application traffic for 10,000+ concurrent users and ensuring high availability.
* Developed and implemented ACLs and NAT rules on routers and firewalls, regulating traffic flow for 3 data centers and improving overall network security posture.
* Deployed content filtering solutions using Blue Coat and Websense, blocking 10,000+ non-business or malicious URLs monthly, improving employee productivity and reducing phishing risks.
* Supported the implementation of Palo Alto PA-5000, Cisco ASA, and Check Point MDM firewalls across 10+ enterprise and remote office locations, standardizing security policies globally.
* Authored and maintained security documentation including SOPs, MOPs, and incident response workflows, reducing incident response time by 20% and improving operational efficiency.
* Participated in policy enforcement, compliance audits, and risk assessments for the Defense Research Engineering Network (DREN), achieving full adherence to DoD security standards.
* Served as lead engineer for IPS evaluation and integration, collaborating with DISA and DoD teams to implement IPv6-ready security coverage across enterprise networks.
* Managed Blue Coat SG appliances for secure web content filtering, maintaining logs to support over 100 internal investigations and regulatory compliance audits.
* Monitored and resolved NSM alerts using Indeni 8.5, nCircle 7.9, and EM7 10.2, maintaining 99.9% uptime and reliability across multi-site enterprise and data center networks.
* Designed and deployed advanced firewall configurations, VPN tunnels, and cloud-integrated network services with Qualys and other security products to reinforce LAN security and business continuity, while aligning with ITIL-based problem management and global enterprise technical standards.

**Environment:** Implemented load balancing and traffic control using F5 BIG-IP LTM 15.1 and GTM 15.1, secure access via Cisco ISE 2.7 and Blue Coat ProxySG 10.5, and used tools like Splunk 9.1, Tufin Orchestration Suite 22.1, Nessus 10.3, and ServiceNow San Diego for monitoring, auditing, and vulnerability management.

**Virtusa, Southborough, MA June 2019 to Aug 2020**

**Firewall Engineer**

**Responsibilities:**

* Performed upgrades and migrations of Check Point firewalls from Gaia R77.10 to higher stable releases, completing 20+ major upgrades with minimal downtime (<30 minutes) and maintaining full configuration backups for 50+ production firewalls.
* Maintained High Availability (HA) clusters for Check Point firewalls using SmartConsole and ClusterXL, achieving 99.99% uptime across production environments and supporting critical services for 15,000+ users.
* Designed and implemented secure firewall policies and rules across Check Point, Cisco ASA, Fortinet, and Palo Alto platforms, protecting over 15,000 endpoints and preventing unauthorized access to enterprise applications.
* Administered and optimized Fortinet firewalls using FortiManager 7.2, FortiAnalyzer 7.2, and FortiClient 6.4, ensuring compliant traffic flows and reducing security incidents by 25% across multi-site networks.
* Integrated LDAP and Microsoft Active Directory 2016 with Check Point for user identity awareness, providing role-based access control for 5,000+ employees and contractors.
* Configured and maintained IPSec and SSL VPNs using Cisco ASA, Fortinet, Palo Alto, and Check Point, supporting secure remote connectivity for 2,000+ remote users across 10+ branch offices.
* Upgraded, patched, and maintained firewall firmware and OS across all platforms quarterly, remediating 150+ vulnerabilities and improving overall enterprise security posture.
* Backed up and restored Check Point and Fortinet firewalls during scheduled maintenance and prior to major configuration changes, ensuring zero configuration loss and fast recovery times (<15 minutes).
* Migrated policies and configurations from Palo Alto to Cisco ASA firewalls, achieving zero policy conflicts and uninterrupted services for 3 mission-critical enterprise applications.
* Enforced network access policies by configuring and monitoring security rules based on user identity, device type, and access location, reducing unauthorized access incidents by 30%.
* Used TCPDUMP, packet captures, and log analysis to investigate complex firewall-related traffic and performance issues, resolving 95% of issues within SLA and minimizing downtime.
* Troubleshot High Availability failover issues, ensuring real-time synchronization between cluster members and reducing failover-related downtime to under 5 minutes.
* Configured Site-to-Site VPN tunnels for third-party and branch office connectivity using static routes and phase 1/2 negotiation, supporting secure communications for 10+ partner and branch sites.
* Supported DLP (Symantec Endpoint Protection) deployments across 5,000+ endpoints and integrated network gateways, reducing data leakage incidents by 20% within 6 months.
* Monitored firewall performance and usage patterns, providing trend reports and alerts via SmartReporter and FortiAnalyzer, enabling proactive capacity planning and performance optimization for enterprise networks.
* Integrated WAF solutions with firewall appliances to protect 50+ web applications against Layer 7 threats, reducing application-layer attacks by 40%.
* Collaborated with internal teams to deploy firewalls in staging, production, and DR environments, following MOP/SOP procedures and completing 10+ major deployments on schedule with zero service interruptions.
* Managed network performance and system uptime across large enterprise data centers and wide area networks by leveraging analysis tools such as Opnet, conducting proactive performance metric monitoring, and leading configuration upgrades to support evolving business technology needs.
* Administered end-to-end lifecycle support for project-based infrastructure initiatives, including configuration management, documentation of technical standards, and hands-on troubleshooting to resolve connectivity and system performance issues across distributed business systems and hybrid cloud environments\

**Environment:** Palo Alto Networks PAN-OS 8.1.6-h2, Panorama 8.1.6-h2, Expedition 2.x, Check Point R81, Fortinet FortiGate 7.4.7, FortiManager 7.4.7, Cisco ASA 9.1, Cisco ISE 3.2, Aruba ClearPass 6.9.0, Juniper SRX550, F5 BIG-IP TMOS 15.1.10, F5 ASM 15.1.10, Blue Coat Proxy SG 6.x, Cisco Secure Firewall ASA 9.23.

**DXC Technology, Ashburn, VA March 2017 to May 2019**

**Network Engineer**

**Responsibilities:**

* Configured and managed enterprise firewalls including Palo Alto, Cisco ASA, and Check Point for perimeter and internal segmentation, ensuring secure access control and threat prevention.
* Designed and troubleshot Site-to-Site and Remote Access VPN tunnels using Cisco ASA, Palo Alto, and Check Point devices for secure third-party and branch connectivity.
* Reviewed and optimized firewall rulebases using Tufin and Splunk, identifying unused and shadowed rules to improve policy performance and audit readiness.
* Deployed and maintained intrusion detection and prevention systems (IDS/IPS) including Cisco Sourcefire and Firepower, customizing signature policies and monitoring alerts.
* Implemented URL filtering and content inspection using Websense and Bluecoat Proxy SG to enforce secure web usage policies across business units.
* Supported Web Application Filtering and Application Control on firewalls and proxies to mitigate risk from malicious sites and unsanctioned applications.
* Performed IOS and firmware upgrades on Cisco routers, ASA, FWSM, and F5 devices, ensuring minimal downtime during maintenance windows.
* Conducted NAT and ACL configurations on routers and firewalls to securely connect internal networks with external resources and business partners.
* Installed and managed F5 LTM/GTM appliances including virtual servers, health monitors, SNATs, and iRules for traffic distribution and HA architecture.
* Coordinated vulnerability management using tools like Nessus, reviewing scan reports and applying critical patches to harden network infrastructure.
* Configured and monitored Cisco ISE and NAC for network access control based on 802.1X, EAP-TLS, and device profiling, improving endpoint compliance.
* Investigated network security incidents, analyzed logs, and performed packet captures using Wireshark, TCPDump, and SmartView Tracker.
* Implemented AAA solutions using FreeRADIUS, Cisco ACS, and ISE to centralize user authentication, authorization, and accounting across network devices.
* Created and updated detailed Method of Procedures (MOPs), runbooks, and technical documentation for changes, audits, and compliance checks.
* Participated in enterprise change control processes, ensuring proper risk assessment and rollback planning for all security-related implementations.
* Provided Tier 2/Tier 3 operational support for LAN/WAN and data center infrastructure, resolving complex network security and connectivity issues.
* Worked with DISA and DoD security teams on live testing, evaluation, and integration of IPv6-capable Intrusion Prevention Systems for the DREN backbone.
* Managed ACLs and firewall filters on Cisco and Juniper routers/firewalls to enforce segmentation between sensitive and general-purpose networks.
* Administered secure access to Active Directory resources by adjusting GPOs, user groups, and enforcing security baselines.
* Deployed IPsec VPN and SSL VPN configurations with encryption domains, hashing algorithms, and security associations on Check Point firewalls.
* Collaborated with compliance teams for FISMA, NIST, and Privacy Act alignment, supporting CNDSP certification and IA vulnerability remediation.

**Environment**: Worked with Check Point R77.30/R80.10, Palo Alto PA-3000 series, and FortiGate 100D/300D for perimeter security and Utilized Cisco ISR 2900/3900 routers, Catalyst 2960–6500 switches, and ASA 5500-X firewalls in enterprise networks.

**Itransition, Decatur, GA Sep 2015 to Feb 2017**

**Network Engineer**

**Responsibilities:**

* Designed, implemented, and maintained LAN/WAN infrastructures, including configuring Cisco routers (7600, 7200, ASR 9000) and switches (Nexus 7000/5000/2000, Catalyst 2960/3550/3750), supporting 5,000+ end-users across 10+ enterprise locations.
* Installed and configured Cisco ASA 5500 series and Juniper SRX firewalls, reducing security incidents by 35% and maintaining 99.9% network uptime.
* Managed and deployed OSPF, EIGRP, BGP, and RIP routing protocols, optimizing internal and external routing, reducing network latency by 15%, and improving convergence times.
* Configured VLANs, trunking, and inter-VLAN routing across multiple switch models, segmenting 200+ departments to enhance security and manage traffic efficiently.
* Monitored network performance and troubleshot connectivity issues across routers, switches, firewalls, and load balancers, reducing downtime by 20% and improving MTTR using SolarWinds and Netcool.
* Implemented VPN solutions (IPSec, SSL) between multiple remote offices and HQ using Cisco ASA, Palo Alto, and Juniper SRX, providing secure access to 2,500+ remote users.
* Managed and maintained MPLS backbone, including PE-CE configurations and MPLS Traffic Engineering, improving WAN reliability by 25% and supporting critical business applications.
* Provided L3 support for over 40,000 network devices across datacenters, operations, corporate, and DR environments, resolving 95% of critical incidents within SLA.
* Led migration of network infrastructure to MPLS WANs, replacing legacy point-to-point circuits, enhancing redundancy, and implementing BGP for dynamic failover.
* Installed and managed F5 BIG-IP LTM load balancers, including iRule development, SSL offloading, and traffic optimization, supporting high-availability applications serving 10,000+ users.
* Configured Cisco Unified Communications Manager and deployed VoIP services, including Cisco IP phones and analog endpoints, improving call quality by 20% and reducing PSTN costs by 18%.
* Conducted network assessments, capacity planning, and documented detailed network topologies using Microsoft Visio, supporting strategic upgrades across 5+ data centers.
* Deployed and maintained Symantec AV, IBM QRadar SIEM, and Bluecoat ProxySG for monitoring and content filtering, increasing threat detection efficiency by 30%.
* Created and managed ACLs, route maps, and NAT rules to secure data flow across critical paths, preventing unauthorized access to 100+ sensitive systems.
* Installed and maintained DHCP and DNS services using Cisco routers and VitalQIP in high-availability environments, ensuring uninterrupted services for 24/7 operations.
* Troubleshot L2/L3 network issues using Wireshark, tcpdump, SNMP, SolarWinds, and Netcool, reducing mean time to resolution (MTTR) by 30% across enterprise environments.
* Built and managed VMware virtual networks and supported VM connectivity across data centers using Cisco Nexus, enabling seamless migrations and 99.99% uptime.
* Collaborated on data center buildouts and migrations, including subnet movement, firewall rule audits, and policy migrations, completing projects 15% ahead of schedule.
* Implemented STP, RSTP, and VTP for loop prevention and stable topology in large-scale switched environments, reducing broadcast storms by 40%.
* Applied Quality of Service (QoS) policies to prioritize business-critical applications and voice/video traffic, improving application performance by 25% and VoIP quality by 20%.
* Automated repetitive tasks and network configurations using Python scripting and REST APIs, saving 50+ engineering hours per month and reducing configuration errors by 35%.
* Participated in network change management, including configuration backups, scheduled upgrades, and rollback procedures, maintaining ITIL compliance and minimizing risk for 100+ critical systems.
* Collaborated with global teams and cross-functional stakeholders to gather infrastructure requirements, evaluate IT costs, and execute enterprise network integration strategies—ensuring technical solutions aligned with strategic business goals, customer experience standards, and IT service continuity.

**Environment:** Worked in a multi-vendor enterprise network using Cisco ASR 9000, Catalyst 6500, Nexus switches, and Juniper SRX/MX series devices and configured and supported BGP, OSPF, MPLS, IPsec VPNs, VLANs, QoS, NAT, ACLs, HSRP/VRRP, and integrated F5 load balancers for HA.