

Professional Summary

- Network and Security Engineer with 4+ years of hands-on experience in enterprise and hybrid cloud environments, specializing in designing, securing, and troubleshooting on-prem and cloud networks with a strong foundation in IP networking, routing, firewalls, and automation.
- Proven ability to take ownership of complex security issues end-to-end, collaborate with cross-functional teams, and support large-scale, SLA-driven production infrastructures aligned with Microsoft cloud and enterprise security standards.

Core Competencies

- **Firewall Technologies:** Palo Alto NGFW, Panorama, Cisco Firepower, FortiGate, Check Point, Prisma SD-WAN, App-ID, User-ID, MACSec, SSL Decryption, NAT, High Availability.
- **Cloud & Virtualization:** Hybrid Cloud Network Design, Microsoft Azure, AWS, VMware ESXi, On-Prem and Cloud Integration.
- **Networking & Protocols:** IP, TCP/UDP, ARP, DNS, DHCP, HTTP/HTTPS, Routing & Switching, OSPF, BGP, EIGRP, MPLS.
- **Automation & Configuration Management:** Ansible (YAML), PowerShell.
- **Load Balancing & Availability:** Application Load Balancing (LTM/HLB), High Availability, Resilient Network Design.
- **Datacenter & Storage:** Large-Scale Datacenter Environments, Enterprise NAS & SAN.
- **VPN:** GlobalProtect, IPsec VPN, SSL VPN, GRE.
- **Operations & Tools:** OSI Layer 2–7 Troubleshooting, Packet Analysis (Wireshark), Incident Response, Root Cause Analysis (RCA), Vulnerability Assessment, ITIL, ServiceNow, JIRA, Salesforce.

Experience

- **Senior Associate – Cybersecurity Consultant** **Infosys Limited**
Jun 2025 – Present | Client: Mercedes-Benz (Daimler AG)
 - Delivered end-to-end cybersecurity consulting including problem analysis, effort estimation, firewall architecture design, and deployment across enterprise environments.
 - Provided L2/L3 support for multi-vendor firewalls (Palo Alto, FortiGate, Check Point, Cisco Firepower), managing security policies, NAT, VPNs, upgrades, and high-availability configurations.
 - Led POCs for firewall and cloud security solutions, conducted vulnerability assessments, and implemented security hardening for 24x7 SLA-driven production systems.
- **Network Security Engineer – Escalation Engineer** **iOPEX Technologies Pvt. Ltd.**
Jan 2022 – Jun 2025
 - Served as L3 escalation engineer for enterprise-scale Palo Alto NGFW deployments, resolving high-severity network and security incidents within strict SLA targets.
 - Designed, deployed, and supported secure hybrid cloud architectures across Azure, AWS, and VMware ESXi, including advanced troubleshooting of GlobalProtect, IPsec/SSL VPNs, GRE, MACSec, and routing (BGP, OSPF).
 - Built and operated replication lab environments to isolate OS-level defects, performed deep packet inspection using Wireshark, and delivered 1000+ enterprise security solutions across large datacenter environments.
 - Designed and supported high-availability firewall and application load-balancing (LTM/HLB) architectures, automated workflows using Ansible and PowerShell, and mentored junior engineers.

Education

B.Tech in Electrical & Electronics Engineering

2017–2021

Guru Gobind Singh Indraprastha University, New Delhi, India

Certifications & Awards

- Palo Alto Networks Certified Network Security Engineer (PCNSE) — 2024
- RISE Award – Certificate of Excellence — Infosys & Mercedes-Benz, Q2 FY25
- Best Productivity Award — iOPEX Technologies, Q4 FY24
- Top Performer – TAT NGFW — iOPEX Technologies, Q4 FY23
- Best Productivity Award — iOPEX Technologies, Q3 FY23