

SHEHROZ ARIF

✉ shehroz.arif@hotmail.com ☎ 773-379-5951 🔗 LinkedIn



Senior Network & Security Engineer | OT/IT Security |
No VISA Sponsorship Needed

PROFESSIONAL SUMMARY:

- Senior Network & Security Engineer with **9+ years of experience** designing, implementing, troubleshooting, and securing enterprise, data center, OT/IT, and hybrid cloud infrastructures. Strong hands-on expertise in **Palo Alto Networks/Panorama, Fortinet FortiGate, Cisco FTD/FMC, Juniper SRX, Cisco ISE, F5 LTM/ASM, Azure, and AWS**, with advanced experience in BGP/OSPF routing, switching, IPSec/SSL VPN, ExpressRoute, SD-WAN, NAT, Zero Trust/NAC, and Layer 2–7 troubleshooting across on-premises and cloud environments, including network security, DNS, firewall, VPN, application connectivity, incident response, and security compliance.

CERTIFICATIONS:

- NSE4 | NSE5 | NSE7 | PCNSE | CCNP Enterprise | CCNP Security | Azure Networks | ITIL Foundation

KEY ACHIEVEMENT:

- Led a cross-functional team of 8 engineers to deploy Palo Alto NGFWs and Fortinet firewalls, securing 1,000+ endpoints and reducing lateral threat movement by 35%.
- Reduced critical vulnerabilities by 40% through proactive monitoring and vulnerability management using Nessus, FortiAnalyzer, and Cisco Stealthwatch.
- Spearheaded a multi-site Azure ExpressRoute deployment, coordinating with Microsoft, Lumen, and internal stakeholders to establish reliable hybrid connectivity between on-premises and Azure environments.
- Established a Network & Security Training Program, mentoring 50+ internal engineers and 500+ students in CCNA, networking, and cybersecurity, achieving a 90% certification success rate.
- Implemented a 24/7 SOC monitoring framework by integrating Splunk, FortiSIEM, and Palo Alto Cortex XSOAR, reducing incident response time by 45%.
- Served as a Cisco Certified Networking Instructor, delivering CCNA networking and security training.

TECHNICAL SKILLS:

Routing & Switching	BGP, OSPF, EIGRP, IS-IS, TCP/IP, IPv4/IPv6, VLANs, STP/RSTP, HSRP, VRRP, LACP, EtherChannel, Trunking, Inter-VLAN Routing, Route Redistribution, Policy-Based Routing (PBR), High Availability (HA)
Firewalls & Security	Palo Alto NGFW, Panorama, Fortinet FortiGate, FortiManager, FortiAnalyzer, Cisco ASA, Cisco FTD, Cisco FMC, Juniper SRX, Check Point, FortiWeb, Security Policies, ACLs, NAT/PAT, IPS/IDS, Application Control, Network Segmentation, Micro-Segmentation, Zero Trust, Vulnerability Management
Network Security	VLAN Hooping, DHCP Snooping, Arp Spoofing, MAC Flooding, Man-in-the-Middle, Password Cracking, STP Attacks, SSL/SSH Interception, Zero Trust, NGFW, NAC, Vulnerability Management, SIEM, SOC, Compliance, Threat Hunting, DLP
Cloud & Hybrid Networking	Microsoft Azure, AWS, Azure ExpressRoute, Azure Firewall, Virtual Networks (VNet), VNet Peering, Network Security Groups (NSG), User Defined Routes (UDR), Route Tables, Load Balancers, Private Endpoints, Private DNS, Application Gateway, Hybrid Cloud Connectivity
Cisco & Data Center Technologies	CISCO Routers 1700, 1800, 2500, 2600, 2800. CISCO High-End Router 3600, 3800, 7200. CISCO Switches 1900, 2950, 2960. CISCO Campus Switches 3550XL, 4984 Core Catalyst 4503, 4507RE, 6500/6503/6507/9606R, CISCO WLC 2504, 3504, 4402, 5508, 5520, 9800 WLC and Wireless Access Point.
VPN & Secure Connectivity	IPSec, IKE/IKEv2, Site-to-Site VPN, Remote Access VPN, SSL VPN, DMVPN, SD-WAN, Azure VPN, Hybrid Cloud VPN, SSL/TLS, SSH
Identity & Network Access Control	Cisco ISE, RADIUS, TACACS+, 802.1X, Active Directory, LDAP, SAML, Digital Certificates, Network Access Control (NAC), Role-Based Access Control (RBAC)
Monitoring & Troubleshooting	Wireshark, SolarWinds, PRTG, FortiAnalyzer, Panorama, Palo Alto Traffic/Threat Logs, Packet Capture, Syslog/Rsyslog, Nagios, LogicMonitor, ServiceNow, Network Performance Monitoring, Root Cause Analysis

Servers	Domain servers, DNS servers, WINS servers, Mail servers, Proxy Servers, Print Servers, Application servers, FTP servers, Avocent Console server, DNA center
Operating Systems	Linux, UNIX, Windows Server, Active Directory
OT/IT & Security Frameworks	OT/ICS Security, Network Segmentation, NIST, CIS Benchmarks, PCI-DSS, HIPAA, IEC 62443, NERC-CIP
Automation & Infrastructure	Terraform, Infrastructure as Code (IaC), Network Automation, Configuration Management

Sr. Network Engineer
F5 Networks, Seattle, WA

February 2026 – Present



Responsibilities:

- Manage and troubleshoot a global network security environment of **100+ Palo Alto Networks firewalls**, with approximately **80 firewalls centrally managed through Panorama HA**, supporting data centers, branch offices, cloud environments, and business-critical services.
- Provide advanced **Layer 3–7 network and firewall troubleshooting** for production incidents involving **BGP, routing, route propagation, asymmetric traffic, NAT, DNS, TCP/SSL, security policies, application connectivity, and VPNs**, using packet captures, session analysis, traffic logs, and CLI diagnostics for root-cause analysis.
- Administer and troubleshoot **Palo Alto Panorama**, including Device Groups, Templates, VSYS, shared/inherited security policies, NAT and security rules, address/service objects, configuration validation, commits, policy pushes, and configuration synchronization.
- Troubleshoot **Azure and hybrid cloud networking**, including VNets, VNet Peering, NSGs, UDRs/route tables, effective routes, Azure Firewall, Load Balancers, Private Endpoints, Private DNS, Application Gateway, and connectivity between **Azure, AWS, Oracle Cloud and on-premises environments**.
- Troubleshoot **site-to-site IPsec VPNs and hybrid connectivity**, validating IKE/IPsec negotiation, tunnel status, routing, NAT, security policies, DNS resolution, and bidirectional traffic flows across enterprise and cloud environments.
- Perform advanced **DNS and application connectivity troubleshooting**, including Private DNS, conditional forwarding, split-horizon DNS, TCP resets, SSL/TLS traffic, application timeouts, and end-to-end packet-flow analysis across distributed environments.
- Support firewall lifecycle and infrastructure changes including **Panorama onboarding, policy migrations, firewall decommissioning, configuration cleanup, duplicate object remediation, hardware refreshes, and deployment of Palo Alto PA-5200/PA-5400 series platforms**.
- Conduct **SOX firewall security rule reviews and policy governance**, identifying unused, duplicate, temporary, overly permissive, and obsolete rules while validating business requirements and remediation activities.
- Integrated network infrastructure changes into CI/CD pipelines to automate configuration deployment, validation, compliance checks, and operational tasks.
- Work with **Linux and Terraform-based network/cloud environments**, using CLI troubleshooting and reviewing existing infrastructure configurations to diagnose routing, DNS, TCP connectivity, and cloud network issues.

Sr. Network Engineer
Sound Transit, Seattle, WA

January 2025 – January 2026



Responsibilities:

- Designed, deployed, and supported **Juniper SRX4200 firewall clusters**, implementing security policies and **IPsec VPN tunnels** to provide secure connectivity across enterprise and transit environments.
- Configured and supported **Palo Alto and Fortinet NGFWs**, implementing application-based security policies, network segmentation, and advanced controls across train stations and enterprise networks.
- Supported **Azure ExpressRoute and hybrid cloud connectivity** as part of the Core Cybersecurity team, configuring and troubleshooting **BGP routing** between on-premises infrastructure, service providers, and Microsoft Azure, along with traffic-log integration into SIEM for monitoring.
- Deployed and supported **Azure-to-on-premises VPN connectivity** for the **EDP Pilot and Databricks environments**, troubleshooting IPsec, routing, security policies, and end-to-end network connectivity.
- Implemented and supported **Cisco ISE Network Access Control (NAC)** and Cisco Secure Wireless, enabling endpoint profiling, role-based segmentation, and secure network access across enterprise and transit environments.

- Provided advanced **network and security troubleshooting** across routers, switches, firewalls, wireless access points, VPNs, and cloud connectivity, performing root-cause analysis using **Wireshark, Intermapper, device logs, and CLI diagnostics**.
- Developed network automation and configuration-management workflows using **scripting, APIs, Infrastructure as Code (IaC)**, and standardized configuration templates.
- Administered and supported enterprise network infrastructure across **Cisco, Aruba, F5, Palo Alto, and Versa Networks**, ensuring availability, performance, security, and operational stability.
- Supported security and segmentation requirements for transportation and payment environments, applying **IEC 62443, PCI-DSS, SSL/TLS, IPsec, and SSH security controls**, while developing security runbooks and incident-response procedures.

Sr. Network Engineer

July 2024 – December 2024

Olympus of Americas, Center Valley, PA

Responsibilities:



- Designed, deployed, and supported enterprise **LAN/WAN and network security infrastructure** across data centers and branch locations, managing **Cisco Catalyst 9600/6500/4500/9300 and Nexus 7K/9K** platforms with VLANs, STP, trunking, inter-VLAN routing, and high-availability configurations.
- Configured and managed **Palo Alto and Fortinet NGFWs**, Fortinet WAF policies, security rules, NAT, and network segmentation to protect critical applications and enterprise traffic.
- Engineered and troubleshooted **BGP, OSPF, and EIGRP** routing environments, including migration from EIGRP to OSPF, BGP peering with service providers, route optimization, **QoS, and policy-based routing (PBR)**.
- Implemented secure connectivity solutions using **IPsec VPN, SSL VPN, DMVPN, and SD-WAN**, supporting encrypted connectivity between remote sites, branch offices, and enterprise networks.
- Configured **Cisco ISE Network Access Control (NAC)** with endpoint profiling, **RADIUS/TACACS+, role-based access policies, and Zero Trust segmentation**, integrating network access and security controls across the enterprise.
- Deployed and supported **Cisco WLC 9800 and Cisco 9120/4800/3800 wireless infrastructure**, integrating wireless access with **Cisco ISE** for secure endpoint onboarding, profiling, and policy enforcement.
- Performed end-to-end network and security troubleshooting using **Wireshark, FortiAnalyzer, SolarWinds, and SIEM platforms**, analyzing routing, firewall, VPN, and application traffic while supporting high-severity incidents and 24x7 operations.
- Supported **IoT/OT network integration, security compliance, and change management**, collaborating with cybersecurity, facilities, and engineering teams while developing **HLDs, LLDs, security runbooks, risk assessments, and backout plans** for production changes.

Sr. Network Security Engineer

January 2020 - June 2024

Barclays, Seattle, WA

Responsibilities:



- Designed, implemented, and supported **enterprise network and security infrastructure** across data centers, branch locations, and hybrid cloud environments, ensuring secure and highly available connectivity for business-critical services.
- Deployed and managed **Palo Alto NGFWs/Panorama and Cisco FTD/FMC**, implementing application-aware security policies, **NAT, IPS/IDS, network segmentation, and threat-prevention controls** across enterprise environments.
- Managed and optimized **F5 ASM/WAF** to protect critical web applications against **OWASP Top 10 vulnerabilities and application-layer threats**, supporting secure delivery of business-critical applications.
- Configured and maintained **Cisco ISE Network Access Control (NAC)**, implementing endpoint profiling, role-based access, network segmentation, and **Zero Trust security policies** across enterprise networks.
- Deployed and troubleshooted **IPsec, SSL VPN, and site-to-site VPN connectivity**, supporting secure communication between data centers, branch locations, remote users, and hybrid environments.
- Managed and optimized **Azure ExpressRoute** connectivity between on-premises infrastructure and Azure, supporting secure and resilient **hybrid cloud networking** and troubleshooting end-to-end connectivity issues.
- Integrated and analyzed **firewall, VPN, WAF, and ISE logs** across SIEM and security monitoring platforms, using **Nessus, FortiAnalyzer, Wireshark, and SolarWinds** for vulnerability assessment, packet analysis, threat monitoring, and root-cause troubleshooting.

- Supported **SOC operations, incident response, and security investigations**, analyzing firewall logs, packet captures, vulnerabilities, and security events while coordinating remediation and aligning controls with **NIST, PCI-DSS, and HIPAA** requirements.
- Developed and maintained **HLDs, LLDs, security runbooks, and operational procedures**, supporting firewall standardization, incident response, network changes, compliance activities, and **micro-segmentation/Zero Trust** initiatives.

System Network Engineer

Nokia, Dallas, TX

Responsibilities:

January 2017 - November 2019



- Provided on-site support for **data center operations** and **security monitoring**, ensuring availability, integrity and protection of enterprise infrastructure.
- Configured and maintained **Cisco switches, routers and firewalls**, enabling secure LAN/WAN connectivity and inter-site communications.
- Managed and monitored **Palo Alto NGFWs, Cisco ASA/FTD and Fortinet NGFWs** to enforce security policies, control application-level traffic and ensure secure application delivery.
- Deployed and supported **IPsec** and **SSL VPN solutions** to secure connectivity for remote users and branch locations.
- Worked closely with the **SOC team** to monitor security events, investigate anomalies and escalate critical alerts based on severity.
- Integrated firewall and VPN logs into **syslog servers**, enhanced visibility for **threat detection** and **incident response**.
- Conducted **packet-level traffic analysis** using **Wireshark** to investigate suspicious network activity and performance issues.
- Assisted in **vulnerability assessments** and remediation efforts using **Nessus** reports, collaborating with internal teams to address identified risks.
- Configured and optimized **routing protocols** including **OSPF** and **BGP**, ensuring secure and stable traffic flows between enterprise environments.
- Applied **SSL/TLS encryption, IPsec tunneling** and **SSH hardening** across devices to strengthen perimeter security and endpoint protection.
- Developed and maintained **runbooks, incident response playbooks** and **technical documentation** to streamline SOC processes and ensure compliance readiness.
- Collaborated with cybersecurity teams to enforce access control policies via **Active Directory** integration and implement **multi-factor authentication (MFA)** for privileged accounts.
- Utilized **SolarWinds** and **PRTG** for continuous infrastructure monitoring, alerting and early detection of potential outages.

AWARDS/EDUCATION:

- Master of Science in Information Technology (MSIT)
University of the People
2026 - 2028
- Five Years of Instructor Excellence Award
Cisco Networking Academy
2022
- Bachelor of Science in Computer Science (BSCS)
South City Institute of Management & Technology
2014 - 2018

