

MUHAMMED SHAHEER KP

Network Security Consultant | CISSP Certified | NAC | Firewall & WAF | Zero Trust

+966 548828992 | mshaheerkp@gmail.com | Riyadh, Saudi Arabia | linkedin.com/in/muhammed-shaheer-kp | SEC Registered

PROFESSIONAL SUMMARY

CISSP-certified Network Security Consultant with 14+ years across networking and cybersecurity, architecting and operating multi-vendor security for government, banking and critical-infrastructure organisations in Saudi Arabia. Hands-on across the Fortinet Security Fabric (FortiGate firewall, FortiWeb WAF, FortiSandbox, FortiAnalyzer, FortiManager), Palo Alto NGFW, Forescout NAC, Ivanti NAC & VPN, F5 BIG-IP and Splunk SIEM, and integrates complementary platforms including Opinnate network security policy management, Seclore DRM and Riverbed APM. Delivered a 14-appliance, multi-region Forescout deployment covering 10,000+ IT/IoT/OT endpoints and 802.1X/MAB NAC across 300+ bank branches at 99.99% availability. Combines a deep networking foundation from Juniper Networks and Pulse Secure (Ivanti) with customer-facing experience in Zero Trust design, proofs of concept, solution sizing and knowledge transfer.

CORE SECURITY EXPERTISE

NAC & Access Control: Forescout NAC (CounterACT) architecture, deployment & operations · 802.1X & MAB · device discovery, profiling & classification · policy creation & enforcement · dynamic VLAN / ACL assignment · automated quarantine & remediation · NAC HA and DC/DR design

IT / IoT / OT Visibility: Unmanaged-device discovery and control for laptops, desktops, VoIP phones, printers, surveillance cameras, NVRs and sensors · graduated access policies for fragile OT devices

Firewall & Network Security: Palo Alto NGFW · FortiGate · rule-base audit & optimisation · SSL inspection · IPS/IDS · sandboxing · risk-based segmentation · Zero Trust enforcement

WAF & Application Delivery: FortiWeb WAF custom rules, tuning & HA · F5 BIG-IP load balancing (multi-tier DC/DMZ, high availability)

Security Architecture & Integration: Multi-vendor security architecture · Opinnate network security policy management · Seclore DRM · Riverbed APM · Ivanti VPN · Netskope (supporting)

Security Integration & Logging: Forescout ↔ Palo Alto / Cisco / AV integration via REST API · NAC-to-Splunk integration (parsers, correlation searches, dashboards) · FortiAnalyzer log analysis

Operations & Consulting: Incident response & tabletop exercises · root-cause analysis · packet-level troubleshooting · migrations with zero/near-zero impact · PoCs, solution sizing, executive reporting, knowledge transfer

CERTIFICATIONS

Security: CISSP — ISC² (2026) · ISC² Certified in Cybersecurity (CC)

NAC: Forescout Certified Professional (FSCP) · Forescout Certified Associate (FSCA) · Forescout Sales Accreditation · Pulse Secure NAC Expert (Ivanti)

Networking & SIEM: CCNP · CCNA (CSCO11668234) · JNCIS-SP (JPR133589) · JNCIA-M · Splunk Power User

In progress: CISA (ISACA) · BeyondTrust PAM · Master's in Artificial Intelligence

PROFESSIONAL EXPERIENCE

Cybersecurity Consultant — Technical Lead

Jul 2023 – Present

Starlink – Trusted Cyber & Cloud Advisor | Riyadh, Saudi Arabia

Consultant delivering network security architecture, NAC and security operations to Saudi government and critical-infrastructure clients.

SPGA — Current Engagement — Saudi Government Authority, 2,000+ users | Multi-Vendor Security Architecture & Operations

- Architect and operate SPGA's integrated, multi-vendor security stack — Fortinet Security Fabric, Palo Alto NGFW, Forescout NAC, Ivanti VPN, F5 BIG-IP and Netskope — aligned with Zero Trust principles and NCA requirements.
- Manage FortiGate and Palo Alto firewalls — policies, security profiles, SSL inspection, IPS/IDS, routing and traffic shaping — with centralised management through FortiManager.
- Audited and optimised the firewall rule base, retiring unused and over-permissive rules to cut it by 35%, shrinking attack surface and improving throughput.
- Integrated Opinnate network security policy management across the firewall estate to centralise policy visibility, analysis and rule-base governance.

- Manage FortiWeb WAF — custom regex-based rules, false-positive tuning, log investigation, Active/Passive HA and firmware upgrades through CAB change control — and lead CVE response for perimeter devices.
- Deployed FortiSandbox across HQ, DC and branches with 24/7 monitoring; enforce daily IOC-based blocking across firewalls and the Netskope proxy.
- Analyse firewall and network logs in FortiAnalyzer, working with the SOC to support rapid incident detection and response.
- Delivered the Forescout professional-services implementation as a high-availability failover cluster, providing continuous endpoint visibility and access control for 2,000+ users.
- Designed a 3-tier F5 BIG-IP load-balancing architecture across internal DC and DMZ for high availability of mission-critical applications.
- Architecting the Seclore enterprise digital rights management (EDRM) deployment with the vendor implementation team to protect sensitive documents beyond the network perimeter.
- Integrated Riverbed application performance monitoring (APM) to give operations and security teams visibility into application performance and latency.
- Plan and execute migrations, upgrades and patching with zero/near-zero business impact; lead weekly SOC governance meetings and refine playbooks using threat intelligence and NCA feeds.

TAHAKOM — Previous Engagement — *Smart Mobility & National Critical Infrastructure* | Forescout NAC

- Designed, deployed and operated an enterprise-wide Forescout NAC platform of 14 CounterACT appliances across multiple KSA regions and sub-regions, giving unified visibility over 10,000+ endpoints in hybrid IT, IoT and OT networks.
- Discovered and classified previously unmanaged assets — laptops, desktops, VoIP phones, printers, surveillance cameras, NVRs and sensors — turning an unknown device population into a reportable asset inventory.
- Built custom Forescout classification rules to identify proprietary equipment and enforce asset-specific baselines; applied graduated, device-specific policies to fragile OT devices instead of blanket enforcement to avoid operational disruption.
- Integrated Forescout with Palo Alto firewalls and Cisco switches for risk-based segmentation, dynamically restricting unauthorised communication between sensitive assets and critical business applications.
- Engineered REST API integrations between Forescout, Palo Alto firewalls and antivirus platforms to drive automated quarantine workflows and reduce reliance on manual response.
- Designed Zero Trust segmentation combining NAC and NGFW controls, reducing unauthorised lateral movement by 85%.
- Led incident response simulations and OT tabletop exercises (unauthorised device connection, malware outbreak, camera hijacking, firmware tampering, IoT compromise); root-cause analysis reduced MTTR by 30%.
- Resolved operational tickets from initiation to closure using Wireshark, tcpdump and CLI tooling for packet-level and log analysis.
- Performed vulnerability assessments and built prioritised remediation plans across core infrastructure.
- Delivered executive dashboards and compliance reports on asset inventory, risk posture and remediation progress; ran knowledge-transfer sessions and documentation for operational handover.

Cybersecurity Resident Engineer

Sep 2020 – Jul 2023

Security Matterz | **Client: Bank Al Bilad** | Riyadh, Saudi Arabia

- Implemented and operated enterprise NAC end to end across 300+ bank branches, enforcing 802.1X for managed endpoints and MAC Authentication Bypass (MAB) with device profiling for ATMs, POS terminals and other unmanaged devices.
- Engineered active-passive high availability between Primary DC and DR with synchronised profiler databases, achieving 99.99% availability.
- Configured dynamic VLAN assignment, ACL enforcement and real-time posture-based quarantine of unknown or non-compliant devices.
- Integrated NAC with Splunk — custom parsers, correlation searches and automated response workflows across 300+ locations.
- Upgraded cluster appliances through critical migration initiatives and took part in BCP failover testing with IT and business units.
- Introduced automated database purging and retention policies, improving licence utilisation and reducing storage footprint by 40% while maintaining audit compliance.
- Achieved 98% SLA adherence for security incident response and ticket resolution, with no security breaches recorded on the banking network during tenure.

Senior Security Solutions QA Engineer

Dec 2016 – Sep 2020

Pulse Secure (Ivanti) | Bangalore, India

- Validated Pulse Secure NAC integrations with FortiGate, Palo Alto and Check Point firewalls and Splunk SIEM for enterprise interoperability.

- Delivered proof-of-concept implementations for enterprise and government customers, including solution sizing and architecture recommendations.
- Analysed customer network topologies and use cases to troubleshoot deployment issues and advise on deployment strategy.
- Built Splunk integration content — dashboards, correlation rules and automated response workflows — for customer deployments.
- Performed security testing with Burp Suite, Nmap and Codenomicon protocol fuzzing. Awarded “Best Performer” by the engineering team.

Senior Network QA Engineer

May 2012 – Nov 2016

Juniper Networks | Bangalore, India

- Validated 802.1X, RADIUS, TACACS+, port mirroring and storm-control features across Juniper EX, MX and SRX platforms.
- Built test automation with the JT framework and Perl, cutting manual testing by 60%; wrote SLAX scripts for Junos operations and compliance checks.
- Built lab topologies (L2/L3 VPN, OSPF, BGP, MC-LAG, RSTP/VSTP) for security testing and customer PoC demonstrations.
- Root-caused security defects in customer escalations; contributed to Junos Node Unifier and produced design documentation from customer requirements.

Senior Software Engineer (Network Security)

Feb 2011 – Apr 2012

Paxterra Software Solutions | Bangalore, India

- Designed and maintained secure LAN infrastructure for a 1,000-user enterprise with VLAN segmentation, ACLs and structured IP addressing.
- Configured RIP, EIGRP and OSPF routing and implemented SNMP/NetFlow monitoring with custom alerting for traffic and capacity analysis.

TECHNICAL SKILLS

Deep hands-on: Forescout NAC / CounterACT · 802.1X · MAB · RADIUS · NAC HA & DC/DR · Ivanti / Pulse Secure NAC · Splunk (SPL, dashboards, correlation)

Strong working: Palo Alto Networks (PAN-OS) · FortiGate (FortiOS) · FortiAnalyzer · FortiManager · FortiWeb WAF · FortiSandbox · F5 BIG-IP · Ivanti VPN · Cisco switching · Juniper EX/MX/SRX (Junos)

Working / integration: Opinnate · Seclore DRM · Riverbed APM · Netskope (proxy, CASB/SWG) · BeyondTrust PAM · Cisco ISE · Check Point (integration testing) · TACACS+ · REST API integration

Networking: Routing & switching · VLANs · OSPF · BGP · EIGRP · L2/L3 VPN · MC-LAG · port mirroring · SNMP · NetFlow

Tools & automation: Wireshark · tcpdump · Nmap · Burp Suite · Codenomicon · Python · Perl · SLAX · TCL · Jenkins

Frameworks: NCA ECC · MITRE ATT&CK · ISO/IEC 27001 · PCI DSS

EDUCATION

Bachelor of Engineering (B.E.) — Anjuman Engineering College, Bhatkal | Visvesvaraya Technological University, Belgaum | 2005 – 2009

ADDITIONAL INFORMATION

Languages: English (Professional) · Arabic (Fluent) · Hindi (Fluent) · Malayalam (Native)

Professional engagement: Saudi Engineering Council (SEC) registered · ISC² chapter member & speaker (Bangalore, Dubai) · Executive Member & IT Wing Lead, Kerala Engineers Forum Riyadh (1,500+ engineers)

Driving licence: Saudi Arabia & India