



Muhammad Waqar

Citizenship Status: Australian Citizen

Security Clearance: NV1

Mobile: +61469770583

VIC 3064 Australia

E-mail: waqar.ne87@gmail.com

LinkedIn: <https://www.linkedin.com/in/muhammad-waqar-4868a646>

Professional Summary

With over a decade of experience specializing in cloud network engineering, I bring deep technical expertise in designing, implementing, and managing secure cloud and hybrid infrastructures. Proficient in technologies like Palo Alto, Checkpoint, and Zscaler, I have a proven track record of deploying advanced cloud security solutions and optimizing network performance across enterprise environments. My focus has been on integrating multi-cloud strategies, ensuring compliance with industry standards, and safeguarding network ecosystems against evolving threats. Skilled in troubleshooting and automation, I excel in incident management, threat mitigation, and delivering resilient, scalable cloud network solutions.

- An analytical mind.
- An ability to learn new technologies quickly.
- Good time management skills.
- An ability to follow processes.
- Strong documentation skills.
- Good communication skills – both written and verbal

Career Highlights and Key Competencies:

- **Palo Alto Firewall Deployments in Cloud and Hybrid Environments:** Led the deployment of Palo Alto firewalls across multi-cloud and hybrid environments, enhancing cloud-native security with robust traffic monitoring and secure access controls.
- **Cloud-Based Threat Prevention Solutions (Palo Alto):** Configured and optimized Palo Alto's Threat Prevention and WildFire services within cloud networks to detect and mitigate advanced threats, including zero-day vulnerabilities, ensuring proactive threat defense.
- **Centralized Security Management with Panorama:** Managed and deployed security policies using Palo Alto Panorama for cloud and on-premises environments, streamlining policy enforcement and enhancing operational efficiency across distributed networks.
- **Check Point CloudGuard Configuration:** Configured and maintained Check Point CloudGuard firewalls for securing workloads in public, private, and hybrid

cloud environments, including advanced VPN solutions and intrusion prevention systems (IPS).

- **Check Point Security Management in Cloud Deployments:** Administered Check Point Security Gateways across cloud architectures, ensuring high availability, efficient traffic flow, and seamless integration with cloud-native services.
- **Zscaler Internet Access (ZIA) for Cloud Security:** Played a key role in deploying and configuring Zscaler Internet Access (ZIA) to enforce cloud-based web security policies and provide secure internet access for globally distributed teams.
- **Zero-Trust Implementation with Zscaler Private Access (ZPA):** Configured and implemented Zscaler Private Access (ZPA) to enable secure, zero-trust remote access to internal cloud-hosted applications, eliminating the need for traditional VPN solutions.
- **Custom Security Policies in Cloud Networks:** Developed and fine-tuned advanced security policies across Palo Alto, Check Point, and Zscaler platforms to ensure comprehensive application-layer control, threat prevention, and compliance within cloud-based infrastructures.

Competencies are:

- **Professional Qualifications:** Cisco Certified Network Associate (CCNA), CCNP Certified Azure Fundamentals, CISSP IN PROGRESS
- **Routing:** BGP, OSPF, EIGRP, HSRP, VRRP, VRF
- **Security:** Experience in configuring and troubleshooting multivendor firewalls including Palo Alto, Cisco ASA, Juniper, Fortinet, Juniper SRX, Checkpoint FW

TECHNICAL SUMMARY

- **Layer 2 (Switching):** Hands-on experience with Cisco and Juniper. Experience in configuring and troubleshooting spanning tree, rapid spanning tree, EtherChannels, QoS, HSRP, VRRP, GLBP.
- **Layer 3 (Routing):** Hands on experience in configuring and troubleshooting EIGRP, OSPF, BGP. Understanding of how to configure MPLS VPNs, MPLS IPsec tunnels works
- **Security:** Experience in configuring and troubleshooting multivendor firewalls including Palo Alto, Cisco ASA, Juniper, Fortinet, Juniper SRX, Checkpoint FW
- **Load Balancer:** Experience with F5 LTM, GTM and Citrix Netscalers.
- **Date Center Switches:** Hands on experience in configuring and troubleshooting Cisco Nexus 7000, 5000, 2000 series switches.
- **QoS:** Practical experience in configuring packet classification, marking, prioritization

of packet using diffserve QoS technology. Have experience on configuring Policing, Shaping, IP Precedence, DSCP, NBAR, QoS group for Enterprise customers.

- **Network Management/Monitoring:** Experience with Cisco Works, CA Spectrum, CatTools, Juniper STRM and Splunk. Also have some experience with Cisco UCS Manager, Cisco ASDM, Cisco Unified Call Manager and Cisco Security Manager (CSM)
- **Cloud:** Practical Experience with configuring EC2 instances, VPCs, Direct Connects, Transit Gateway, VPC Peering, internet gateway in AWS and Express Route Circuits, NSGs in Azure
- **Practical knowledge of Cyber and Cloud Security tools and vendors.**
- **Working knowledge of Cisco ACI, SDN**
- **Network Automation:** Python

Education, Professional Training and Membership:

- 2015-2017- **Master's in computer networks**, Melbourne Institute of Technology
- 2007-2011- BSc Electrical/Electronic Engineering with specialization in Microwaves and Antenna Designing – Comsats University, Pakistan
- **CCNA Certified**
- **CCNP Certified**
- **CISSP IN PROGRESS.....**
- **Azure Fundamentals**
- **Member of Engineers Australia**

GAT Lead - Senior Project Engineer (Networks and Security)

L3HARRIS

June 2025 – Present

Key Responsibilities

- Lead Gateway infrastructure initiatives for a major defence client, ensuring alignment with ISM (Information Security Manual) standards.
- Oversee the end-to-end design, build, and test assurance of secure network gateways, collaborating with cross-functional teams.
- Provide technical leadership and mentorship to assigned peers within the uplift project team.
- Act as the primary point of contact for project planning, risk management, and delivery tracking of secure gateway components.
- Ensure all firewall configurations, rules, and integrations meet stringent security and compliance requirements.
- Coordinate with stakeholders to validate that all deliverables are completed on time and within scope.
- Conduct gateway assurance testing and documentation for audit and certification readiness.

Projects

Secure Gateway Uplift Project – Defence Client

- Spearheaded the transition from legacy F5 firewalls to Palo Alto Networks firewalls, ensuring minimal disruption to operational environments.
- Led the design and implementation of secure firewall policies in compliance with the ISM framework.
- Collaborated closely with cybersecurity, infrastructure, and network engineering teams to deliver a secure and scalable solution.
- Successfully completed multiple migration phases on time, with zero critical defects post-deployment.
- Delivered detailed documentation, test plans, and technical artefacts to support certification and governance processes.

Senior Project Engineer (Networks and Security)

Ethan Group

Aug 2024 – Jun 2025

Key Responsibilities:

- Lead and oversee end-to-end project execution for network security and infrastructure solutions.
- Coordinate with cross-functional teams to deliver projects on time and within budget.
- Manage project documentation, timelines, and deliverables to ensure alignment with client requirements.
- Ensure compliance with industry standards and federal regulations, particularly in secure environments.
- Conduct risk assessments and develop mitigation strategies for network security projects.
- Collaborate with stakeholders to identify and implement system upgrades and enhancements.
- Provide technical expertise in configuring, deploying, and maintaining Cisco switches and network devices.
- Oversee the integration and migration of IPsec VPN tunnels for secure communication between federal clients.
- Ensure the successful installation and commissioning of upgraded CCTV surveillance systems.

Projects:

- **Cisco Switch Refresh:** Spearheading a comprehensive refresh of legacy Cisco switches across multiple sites, focusing on performance enhancement and security compliance.
- **CCTV Cameras Upgrade:** Managing the upgrade of outdated CCTV systems, ensuring enhanced video quality, remote accessibility, and integration with modern surveillance platforms.
- **IPsec Tunnel Deployment:** Designing and implementing secure IPsec VPN tunnels to facilitate encrypted communication for federal clients, adhering to stringent security protocols.
- **Network Security Enhancements:** Driving initiatives to strengthen cybersecurity posture, including firewalls, access controls, and secure network configurations.

Key responsibilities:

- Palo Alto Firewall Administration: Manage the day-to-day administration of Palo Alto firewalls, including configuration of security policies, monitoring traffic, and troubleshooting network security issues to ensure the protection of enterprise infrastructure.
- Threat Prevention and WildFire Configuration (Palo Alto): Implement and maintain Palo Alto's Threat Prevention and WildFire solutions, ensuring real-time threat detection, malware analysis, and automated threat response to safeguard against cyberattacks.
- Zscaler Internet Access (ZIA) Management: Oversee the deployment and configuration of Zscaler's ZIA platform to provide secure internet access for users, enforce content filtering, and protect against web-based threats across distributed network environments.
- Zscaler Private Access (ZPA) Administration: Configure and manage Zscaler Private Access to ensure secure, zero-trust access to internal applications for remote users without the need for traditional VPNs, maintaining a secure and seamless user experience.
- Check Point Firewall Configuration and Management: Administer Check Point firewalls, focusing on the setup, maintenance, and monitoring of security policies, intrusion prevention systems (IPS), and virtual private network (VPN) solutions.
- Security Gateway and VPN Solutions (Check Point): Support the management of Check Point Security Gateways, ensuring optimal performance, availability, and secure traffic flow between internal and external networks through advanced VPN configurations.
- Collaborated on network security projects, empowering operations teams to engage in Cyber Incident Management and implement best practices during potential cyber risk events.
- Administered and maintained Juniper SRX and SSR firewalls, ensuring optimal security and network performance.
- Managed and configured F5 load balancers, optimizing traffic distribution for improved application availability and reliability.

- Oversaw DNS management through the Ultra DNS portal, ensuring accurate and efficient record handling to support seamless network functionality.
- Handled complex network requests, providing in-depth troubleshooting and delivering effective solutions to meet operational requirements.
- Developed and enforced decommissioning guidelines in accordance with government PCI audit policies, maintaining regulatory compliance.
- Documented proxy modifications in Confluence, ensuring accurate and up-to-date records for audit and troubleshooting purposes.
- Ensured that Palo Alto and SMC firewall policies adhered to industry security standards and internal compliance requirements.
- Investigated security incidents by analysing Splunk and firewall logs, providing detailed insights and solutions to relevant stakeholders.
- Utilized Skybox to map firewall rules across various platforms, optimizing rule management and ensuring security policies were consistently applied.
- Developed comprehensive runbooks for the implementation of network security changes, streamlining operational processes and ensuring consistent execution.
- Provided clear guidelines and best practices for analysing security incidents, conducting root cause analysis, and recommending effective remediation strategies.
- Demonstrated extensive knowledge of customer service principles, reinforced by industry training and hands-on experience, delivering professional and effective communication with stakeholders and clients.
- **Azure Networking Experience:** Hands-on experience with Azure networking, including managing cloud architecture and operations within Azure environments to support modern, secure, and scalable network infrastructures.
- **Scripting/Programming Knowledge:** While not directly executing scripts, I have a strong understanding of Python and Bash scripting from a network security perspective. I am well-versed in how scripting is used to automate processes, troubleshoot issues, and streamline network security operations. My knowledge extends to Infrastructure-as-Code (IaC) tools such as Terraform and CloudFormation, allowing me to efficiently work alongside DevOps teams and ensure security protocols are embedded within automated deployments.

Projects:

- Palo Alto Firewall Administration: Manage Palo Alto firewalls to secure enterprise networks.
- Project: Deployed firewalls for a global retail client, securing 200+ branches and enhancing threat control.
- Threat Prevention and WildFire (Palo Alto): Configure Threat Prevention and WildFire for advanced threat detection.
- Project: Reduced malware by 40% for a financial institution through WildFire deployment.
- Zscaler Internet Access (ZIA) Management: Secure internet access and enforce web filtering using ZIA.
- Project: Rolled out ZIA for 5,000 users at a healthcare provider, reducing web-based threats.
- Zscaler Private Access (ZPA) Administration: Manage ZPA for secure remote access to internal applications.
- Project: Implemented ZPA for a tech firm, enabling secure access for 1,000 remote employees.
- Check Point Firewall Management: Administer Check Point firewalls and VPN solutions.
- Project: Configured Check Point firewalls for a manufacturing company, improving global connectivity.
- Security Gateway and VPN (Check Point): Manage Check Point gateways for efficient VPN performance.
- Project: Upgraded gateways for a retail store, optimizing secure communications.
- Network Security Policy Management: Develop policies across Palo Alto, Zscaler, and Check Point platforms.
- Project: Unified security policies for an e-commerce platform, improving operational security.
- Incident Response: Troubleshoot and resolve security incidents using Palo Alto, Zscaler, and Check Point.
- Project: Reduced breach response time by 50% for a telecommunications client.
- Security Auditing and Compliance: Conduct audits to ensure compliance with industry standards.
- Project: Led a compliance audit for a financial institution, ensuring regulatory adherence.

Key Responsibilities:

- Palo Alto Firewall Management: Configure, manage, and maintain Palo Alto firewalls to ensure secure network operations.
- Zscaler Management (ZIA/ZPA): Deploy and manage Zscaler's secure internet access (ZIA) and private access (ZPA) for cloud-based security and remote access.
- Check Point Firewall & VPN Administration: Configure and manage Check Point firewalls, including VPN setups, ensuring secure, efficient connections.
- Security Policy Implementation: Develop and enforce security policies across Palo Alto, Zscaler, and Check Point platforms.
- Incident Response: Troubleshoot and resolve security incidents, ensuring swift containment and minimal downtime.
- Auditing and Compliance: Conduct security audits to ensure adherence to industry regulations and internal policies. Monitoring of Core Data Centre infrastructure and provide required systems uptime as per KPI.
- Be a Part of team responsible to manage all the network operational resources.
- Monitoring & Administration of Systems Ltd. networking infrastructure
- Configuration of new network devices.
- Manage overall functions of I.T Operations for smooth operation of BAU's.

Projects

- Key to a data center refresh including the installation and configuration of **Nexus 7ks and Nexus 9ks** with the use of VDCs, VPC, and OSPF to create an inter-DC layer 2 over layer 3 stretched VLAN deployment.
- Palo Alto Deployment: Secured 200+ branches for a global retail client with comprehensive firewall deployment and traffic control.
- Zscaler Implementation: Enabled secure internet access for 5,000 healthcare users and deployed ZPA for 1,000 remote employees at a tech firm.
- Check Point Global Connectivity: Improved secure connections between global offices for a multinational manufacturing company.
- Unified Security Policy: Rolled out unified security policies for an e-commerce platform, streamlining security across cloud and on-premises environments.
- Incident Response: Reduced breach response time by 50% for a telecommunications client using a combination of Palo Alto and Check Point solutions.
- Compliance Audit: Ensured regulatory compliance for a financial institution through a comprehensive security audit using Zscaler and Check Point technologies.
- Projects such as **WAN migration** and **Customer provisioning** has been accomplished successfully.
- Successfully migrated customers from **Old FortiGATES** Firewall cluster to the **new FortiGATES** Firewalls.

- Responsible for the configuration, deployment, and documentation of multiple new sites.
- Created **RUN BOOK** for various Incidents.
- Successfully upgraded **NetScalers** (HA and Standalone).
- Customer's **network troubleshooting** is being done in a timely manner.
- Provided **level 3** support on call to the customers.
- **Monitoring** tools such as **Science Logic (SCILO)** were being used to identify the device's status and **Fortianalyzer** was used to look out for threats and Logs.
- Successfully identified the **root cause** issues for the customers.
- Successfully created **IPSEC tunnels** and tested them to make sure the tunnel is working properly.
- Managed Firewalls such as **FortiGate, Cisco ASA's, NSX.**
- Customer's devices configuration had been transferred to **Cisco Meraki** over a centralized dashboard and **Meraki firewall** had been managed.

Network Engineer (L2)
2019

June 2018- Sep

Impact Solutionz Pty Ltd, Melbourne

Key Responsibilities:

- **Network Security Monitoring:** Monitor and respond to network security alerts using Palo Alto, Check Point, and Zscaler platforms to ensure secure network operations.
- **Firewall Configuration Support:** Assist in configuring and maintaining firewall rules and policies under the guidance of senior engineers.
- **Threat Detection and Mitigation:** Assist in identifying and addressing security incidents by analyzing logs and threat alerts, using tools like Palo Alto Threat Prevention and Check Point IPS.
- **Remote Access and VPN Support:** Provide technical support for remote access solutions like Zscaler Private Access (ZPA) and Check Point VPN, ensuring secure connectivity for remote users.
- **Troubleshooting:** Resolve Level 2 security and network issues, escalating complex problems to senior engineers when necessary.
- **Security Policy Implementation:** Support the application and modification of security policies across Palo Alto, Zscaler, and Check Point platforms.
- **Network Audits and Reports:** Assist in conducting regular security audits and generating reports on network performance and vulnerabilities.

Network Engineer / IT Analyst

June 2013- Dec 2014

Frontier Communications

Key Responsibilities:

- Maintained communication networks, monitored network performance, and resolved any technical issues.
- Collaborated with colleagues on the improvement of network infrastructure to increase quality, reliability, effectively, and reduce expenses.
- Installed and configured network devices, including routers, modems, hubs, switches.

Achievements:

- Technically supported project planning team for development and implementation of proposals and solutions to address hardware and software problems and network emergencies.
- Implemented necessary controls and procedures to protect information system assets from inadvertent modification, disclosure, or destruction.

Network Support Engineer

June 2011- Dec 2013

Zong

Key Responsibilities:

- Monitoring network performance to determine if adjustments need to be made.
- Conferring with network users about solving existing system problems.
- Operating master consoles to monitor the performance of networks and computer systems.
- Coordinating computer network access and use.
- Testing networking software, computer hardware, and operating system software.

Achievements:

- Provided complete end-to-end engineering and installation of route-based IP network solutions.
- Diagnosed network problems involving combination of hardware, software, power, and communications issues.

Additional Skills:

- Configuring RIP, EIGRP, OSPF on IPv4 networks protocols.
- Configuring and troubleshooting of Cisco Switches and Routers: 2960, 3560 series, 1841 routers.
- Implementation and understanding of DHCP, NAT, VLSM, VLANs and WAN.
- Packet Tracer, GNS3, Hyper-V, Wireshark, VM-Ware and MS-office.
- Operating System: Windows Xp, Vista, 7,8.0,8.1,10, Mac OS, and Android.

