

Khaja M

Meriden, Connecticut, United States | k36347259@gmail.com | (475) 477-5811 | [linkedin.com/in/mohammed-khaja-a7b12b279](https://www.linkedin.com/in/mohammed-khaja-a7b12b279)

PROFESSIONAL SUMMARY

Senior Network Engineer with 12+ years of experience in designing, implementing, and optimizing enterprise network infrastructure with a strong focus on network security, firewall technologies, and automation. Proven expertise in deploying and managing Palo Alto Networks firewalls, including advanced security policies, VPNs, and intrusion prevention systems (IPS) to safeguard critical enterprise environments. Hands-on experience providing Level 1/2 IT support for desktops, laptops, and mobile endpoints, managing Windows and Linux servers, and administering cloud server environments across AWS, Azure, and Google Cloud. Skilled in leveraging Ansible and PowerShell scripting to drive automation, streamline configuration management, and improve operational efficiency through automated deployments and patching. Strong background in implementing secure, scalable network architectures aligned with enterprise compliance standards such as SOX, PCI, and NERC CIP. Experienced in supporting large-scale infrastructure projects across diverse environments, ensuring high availability, performance optimization, and secure connectivity. Adept at network security monitoring, troubleshooting complex issues, and collaborating with cross-functional teams to deliver resilient and compliant network solutions aligned with business and operational goals.

WORK EXPERIENCE

Network Architect

Dec 2022 - Present

Exelon, IL

- Provided Level 1/2 support for desktops, laptops, and mobile endpoints, resolving workstation and software issues including installation, upgrade, and maintenance of systems.
- Configured and managed Palo Alto Firewalls to enforce advanced security policies and control inbound/outbound traffic.
- Deployed and administered Panorama for centralized management of multiple Palo Alto Firewalls across environments.
- Managed wind energy projects including turbine selection, site assessment, and performance optimization, improving energy output through advanced modeling techniques and real-time monitoring systems.
- Automated firewall configuration and policy deployment using Ansible to improve operational efficiency.
- Implemented security policies on Palo Alto Firewalls including NAT, security rules, and application-based controls.
- Utilized Panorama to standardize firewall configurations and ensure consistency across all network zones.
- Developed Ansible playbooks for automating firewall rule creation, updates, and compliance checks.
- Performed firewall policy optimization and rule cleanup using Panorama to enhance performance and security posture.
- Integrated Palo Alto Firewalls into enterprise environments ensuring secure segmentation of critical systems.
- Automated configuration backups and firewall provisioning using Ansible for improved reliability.
- Configured advanced threat prevention features on Palo Alto Firewalls including IPS, antivirus, and URL filtering.
- Used Panorama for log aggregation, monitoring, and centralized visibility into firewall activities.
- Automated daily operational tasks such as rule validation and updates using Ansible automation frameworks.
- Implemented role-based access control within Panorama for secure and controlled firewall administration.
- Performed firewall troubleshooting and issue resolution related to connectivity and security enforcement.
- Managed firewall high availability (HA) configurations to ensure uninterrupted network security services.
- Designed and enforced network segmentation using Palo Alto Firewalls to isolate sensitive environments.
- Automated firewall health checks and reporting using Ansible scripts.
- Leveraged Panorama templates and device groups to streamline large-scale firewall deployments.
- Configured site-to-site and remote access VPNs on Palo Alto Firewalls for secure communication.
- Automated compliance validation and audit reporting using Ansible playbooks.
- Conducted feasibility studies for hybrid energy systems combining solar, wind, and battery technologies, delivering cost-effective and reliable solutions for diverse industrial and utility-scale application.
- Monitored firewall logs and security alerts through Panorama to detect and mitigate threats.
- Performed firmware upgrades and patch management on Palo Alto Firewalls using automated Ansible workflows.
- Implemented zero-touch deployment strategies for Palo Alto Firewalls using automation tools.
- Standardized firewall configurations across environments using Panorama-managed templates.
- Automated policy push and configuration synchronization across firewalls using Panorama and Ansible.
- Conducted root cause analysis for firewall-related issues and implemented remediation strategies.
- Configured application-aware traffic policies leveraging Palo Alto's App-ID capabilities.
- Ensured secure access control and traffic inspection using Palo Alto Firewalls in all environments.
- Automated log parsing and reporting for security events using Ansible.
- Managed and optimized firewall throughput and performance using Panorama insights.
- Implemented secure network designs leveraging Palo Alto Firewalls for perimeter and internal segmentation.
- Created reusable Ansible roles for firewall deployment and lifecycle management.
- Enforced compliance standards through centralized policy management using Panorama.
- Collaborated with security teams to implement firewall policies aligned with enterprise standards.
- Automated incident response workflows related to firewall alerts using Ansible.
- Performed continuous monitoring and tuning of firewall policies for optimal security.
- Deployed scalable firewall solutions using Panorama for multi-site environments.
- Maintained documentation for firewall configurations, automation scripts, and security policies.
- Delivered secure, automated, and scalable firewall solutions at Exelon using Palo Alto, Panorama, and Ansible.

Senior Network Security

Jan 2020 - Nov 2022

T-Mobile, NJ

- Provided Level 1/2 support for desktops, laptops, and Android/iOS mobile devices, guiding associates through day-to-day operational processes and shipping and logistics tools.
- Implemented and managed Palo Alto Networks Firewalls to enforce enterprise-wide security policies and protect critical network infrastructure at T-Mobile.

- Configured advanced firewall policies including NAT, security rules, and zone-based segmentation using Palo Alto Firewalls.
- Leveraged Panorama for centralized management of Palo Alto Firewalls, ensuring consistent policy deployment across multiple environments.
- Automated firewall configuration and policy deployment using Ansible, reducing manual effort and improving operational efficiency.
- Developed Ansible playbooks to automate Palo Alto firewall provisioning, rule updates, and configuration backups.
- Implemented firewall rule lifecycle management using automation frameworks to ensure compliance and audit readiness.
- Configured high availability (HA) on Palo Alto Firewalls to ensure uninterrupted security enforcement and failover capabilities.
- Utilized Panorama templates and device groups to standardize firewall configurations and streamline large-scale deployments.
- Automated repetitive firewall tasks such as log collection, configuration validation, and policy audits using Ansible.
- Performed firewall rule base optimization and cleanup on Palo Alto devices to enhance performance and reduce security risks.
- Integrated Palo Alto Firewalls with enterprise authentication systems to enforce identity-based access control.
- Designed and implemented secure network architectures leveraging Palo Alto Firewalls for segmentation and threat prevention.
- Configured advanced threat prevention features including URL filtering, IPS, anti-malware, and application control.
- Used Panorama for centralized logging, monitoring, and reporting to improve visibility into network security events.
- Automated compliance checks and firewall policy validations using Ansible scripts aligned with security standards.
- Supported large-scale firewall deployments and migrations to Palo Alto platforms with minimal downtime.
- Implemented automation-driven configuration management to ensure consistency across firewall environments.
- Troubleshooted complex firewall issues including policy mismatches, NAT conflicts, and connectivity problems.
- Automated backup and restore processes for Palo Alto configurations using Ansible playbooks.
- Worked with cross-functional teams to implement secure access controls using Palo Alto Firewalls.
- Developed automation workflows to accelerate firewall change requests and reduce turnaround time.
- Conducted regular firewall health checks and performance tuning using automated tools and scripts.
- Managed firewall upgrades, patches, and firmware updates using automated deployment strategies.
- Leveraged Panorama to enforce global security policies and maintain centralized governance.
- Implemented role-based access control (RBAC) within Panorama for secure administrative access.
- Automated incident response actions such as blocking malicious IPs and updating firewall rules dynamically.
- Ensured compliance with enterprise security standards through automated policy enforcement and auditing.
- Monitored firewall logs and alerts using Panorama to proactively identify and mitigate security threats.
- Participated in security architecture design discussions focusing on Palo Alto and automation strategies.
- Maintained detailed documentation of firewall configurations, automation scripts, and operational procedures.

Network Engineer

Feb 2017 - Dec 2019

MC Kesson, TX

- Designed and implemented secure enterprise network infrastructure using Palo Alto firewalls, ensuring robust protection of healthcare systems and sensitive data.
- Managed and configured Palo Alto firewall policies including NAT, security rules, and application-based filtering to enforce enterprise security standards.
- Administered Palo Alto Panorama for centralized firewall management, configuration consistency, and log aggregation across multiple sites.
- Implemented site-to-site and remote access VPNs on Palo Alto firewalls to enable secure connectivity across distributed enterprise environments.
- Deployed and optimized firewall security profiles including IPS, Anti-Malware, URL Filtering, and Threat Prevention using Palo Alto platforms.
- Automated firewall configuration and policy deployment using Ansible, reducing manual effort and improving operational efficiency.
- Developed Ansible playbooks for automated provisioning, patch management, and configuration backups of network security devices.
- Led large-scale firewall migrations from legacy platforms to Palo Alto, ensuring seamless transition with zero downtime.
- Performed continuous network security monitoring and log analysis using Panorama to detect and mitigate threats proactively.
- Collaborated with cross-functional teams to design scalable and secure network architectures aligned with enterprise requirements.
- Implemented network segmentation strategies using firewall zones and policies to isolate critical healthcare applications and data.
- Conducted firewall rule audits and optimization to eliminate redundant rules and improve overall security posture.
- Supported infrastructure projects across enterprise environments by integrating firewall solutions into new and existing network designs.
- Managed firewall patching, upgrades, and system updates to ensure compliance with enterprise security policies.
- Developed and maintained detailed documentation for firewall configurations, network diagrams, and security policies.
- Ensured compliance with industry standards such as SOX, PCI, and NERC CIP by implementing strict firewall and access control measures.
- Conducted vulnerability assessments and implemented remediation strategies using firewall-based controls and security best practices.
- Provided advanced troubleshooting for firewall, VPN, and network connectivity issues, ensuring minimal business disruption.
- Configured and managed intrusion prevention systems (IPS) within Palo Alto firewalls to protect against evolving cyber threats.
- Integrated automation workflows to streamline network operations, including configuration management and incident response.
- Participated in change management processes, ensuring secure and compliant deployment of firewall and network changes.
- Collaborated with architecture teams to align firewall and network solutions with long-term enterprise roadmaps.
- Performed capacity planning and performance tuning of firewall infrastructure to support high-availability environments.
- Supported 24x7 network operations by proactively monitoring firewall health, logs, and security alerts.
- Led enterprise network security initiatives focusing on automation, firewall optimization, and centralized management using Panorama.

Network Support Engineer

Jun 2013 - Sep 2016

NTPC Limited, India

- Provided Level 1/2 support for desktops, laptops, and mobile endpoints, resolving workstation and software issues including installation, upgrade, and maintenance of systems.
- Designed and deployed secure vendor VPNs using Juniper MAG Series with dual-factor authentication, leveraging RSA SecurID for robust access control.
- Designed and deployed SIP-enabled unified communications, video conferencing solutions, and voice/data integration across distributed offices.
- Enhanced network performance with optimized LAN, WAN, VLAN, WLAN, and SAN architectures, ensuring redundancy and high availability.
- Managed BGP peering with multiple upstream providers, implementing route dampening and AS path prepending to prevent instability.
- Automated network provisioning workflows by combining Ansible playbooks with Cisco ISE APIs, reducing onboarding time for users.
- Integrated telemetry and analytics platforms with VXLAN fabric to visualize east-west flows and detect anomalies.
- Managed high-availability Palo Alto clusters with session synchronization and stateful failover.

- Configured Juniper vMX and SRX devices in virtualized environments for test automation and lab validation
- Integrated VMS tools with Syslog and SNMP traps for proactive monitoring and alerting of network events.
- Provided Tier 4-level diagnostics using Wireshark, packet captures, and deep protocol inspection tools.
- Configured firewall zones and security profiles aligned with VXLAN VNI mappings for consistent protection policies.
- Optimized SNMP trap forwarding and SolarWinds alert escalation policies to align with ITIL incident management practices.
- Enhanced enterprise routing by deploying EIGRP stub routing in remote branches to limit unnecessary route advertisements.
- Administered Infoblox Grid Manager to centralize IP address blocks, DHCP scopes, and DNS zones for global infrastructure.
- Performed latency, throughput, and jitter analysis on AWS Direct Connect circuits to validate SLA compliance.
- Implemented MPLS CoS (Class of Service) policies for traffic prioritization, ensuring optimal voice and video performance.
- Supported MPLS VPN troubleshooting involving RSVP LSPs, LDP label bindings, and BGP route advertisements.
- Conducted periodic audits of Palo Alto security policies to eliminate redundant rules and improve firewall efficiency.
- Authored detailed network design documentation for LDP, RSVP, and BGP-based MPLS deployments.
- Established P2P redundancy by designing dual-homed connections at critical sites for high availability.
- Applied virtualization and distributed processing techniques to scale conferencing and communication platforms across multiple regions.
- Executed configuration change requests in Cisco ASA 8.4 for client networks, applying ACL and NAT policies to facilitate secure and efficient connectivity.
- Configured routing policies for secure access to mainframes via PC-based emulation tools in SSL/VPN-protected networks.
- Maintained documentation for mainframe access tools integrated with LAN/WAN systems and PC client applications.
- Coordinated site-wide Meraki upgrades, managing resource allocation and reporting status to senior management
- Built foundational scripts in Shell and Python for device inventory and port monitoring.
- Executed ACL/NAT changes on Cisco ASA and Juniper SRX firewalls.
- Participated in PoC projects involving Ansible and Terraform for infrastructure automation.
- Designed and deployed secure vendor VPNs using Juniper MAG Series with dual-factor authentication, leveraging RSA SecurID for robust access control.
- Designed and implemented network segmentation and security policies using VLANs and ACLs for data center traffic isolation.
- Executed configuration change requests in Cisco ASA 8.4 for client networks, applying ACL and NAT policies to facilitate secure and efficient connectivity.
- Managed configuration updates in Juniper SRX 3400 firewalls for internal network segmentation, enhancing network security and performance.
- Deployed and managed high-availability solutions using technologies such as HSRP, VRRP, and GLBP to minimize downtime in the data center.
- Administered URL altering policies through Bluecoat ProxySG's Visual Policy Manager (VPM), ensuring secure and compliant web access
- Provided comprehensive support for network and security systems, troubleshooting issues with the aid of Cisco Prime Infrastructure and Cisco DNA Center.

EDUCATION

JBLET

Bachelor of Technology, Electronics and Communication Engineering

Jun 2008 - May 2012

SKILLS

Programming Languages: Python, Shell

Frameworks & Libraries: Ansible, Terraform

Tools & Software: Palo Alto Firewalls, Panorama, Juniper MAG Series, RSA SecurID, SIP, LAN, WAN, VLAN, WLAN, SAN, BGP, Cisco ISE, VXLAN, Juniper vMX, Juniper SRX, VMS, Syslog, SNMP, Wireshark, SolarWinds, Infoblox Grid Manager, AWS Direct Connect, MPLS, RSVP, LDP, GLBP, HSRP, VRRP, Cisco ASA, Bluecoat ProxySG, Cisco Prime Infrastructure, Cisco DNA Center, Zebra printers, Android, iOS, Azure, Google Cloud, PowerShell, Zabbix, Nagios, ITIL, Agile, Scrum

Cloud Platforms: AWS Direct Connect

CERTIFICATIONS & ACHIEVEMENTS

- Cisco Certified Network Professional (CCNP) - Routing & Switching - Cisco
- Cisco Certified Internetwork Expert (CCIE) - Security - Cisco