RAGHAVENDRA RAO KOLLIPARA

✉ raghavendrarao.kollipara326@gmail.com

☎ (469) 986-8333

📍 Little Elm, TX 75068

RESUME SUMMARY

Experienced Network Security Engineer with over 8 years of expertise in designing, implementing, and managing security solutions across diverse enterprise environments. Proficient in configuring and troubleshooting firewalls, including Palo Alto, Fortinet, Checkpoint, and Juniper, as well as handling VPNs, IDS/IPS, and network segmentation. Skilled in leveraging security management platforms like Panorama, FortiManager, and Firemon for optimization and compliance. Adept at firewall migrations, packet analysis, and threat mitigation, ensuring secure and efficient network infrastructures. Holds a Master's in Electrical Engineering with a focus on Network Security. A proactive problem solver with a strong technical acumen, dedicated to enhancing cybersecurity resilience.

SKILLS

- Active Directory, Advanced Routing, Application Protocols, BGP, Checkpoint, Cisco ASA, Data Center Relocations, DHCP, DNS, Dynamic Routing Protocols, EIGRP, Electrical Engineering, Electronics & Communications, Firewall Administration, Firewall Management, Firewall Migration, Firewalls, Fortinet, Gaia, High Availability Protocols, HSRP, IIS, Installation & Configuration, IOS, IP Address Management, IPSEC, ISAKMP, Layer 2/3, Log Analysis, Malware Detection, Network Infrastructure Management, Network Maintenance, Network Protocols, Network Security, NTP, Operational Readiness Testing, OSPF, Palo Alto, Panorama, Policy Analysis, Policy Creation, Provider-1/MDS, Routing, Security Design, Spanning Tree Protocols, SSL VPN, Switching, Switching Technologies, System Upgrades, TCPDUMP, TCP/IP, Test Case Documentation, Troubleshooting, Troubleshooting User Connectivity, VLANs, VPN, VRRP, VTP, Wireshark,Network security design,Vulnerability assessment,Network access control,Log analysis,Virtual private networks

WEBSITES, PORTFOLIOS, PROFILES

- linkedin.com/in/raghavendra-rao-kollipara-048a3574

WORK EXPERIENCE

City of Virginia Beach - Firewall Engineer
Dallas, TX • 04/2025 - Current

- Designed and implemented firewall policies to enhance network security protocols.
- Monitored network traffic for threats and vulnerabilities using advanced intrusion detection systems.
- Conducted regular audits and assessments of firewall configurations to ensure compliance with industry standards.
- Collaborated with cross-functional teams to troubleshoot and resolve complex security incidents efficiently.
- Evaluated emerging technologies to recommend strategic improvements in network defense mechanisms.
- Led incident response efforts, coordinating with stakeholders to mitigate potential cyber threats effectively.
- Optimized firewall performance through continuous monitoring and fine-tuning of settings and rules.
- With thorough documentation of processes and procedures, ensured smooth handover during staff transitions or absences.
- Actively participated in industry events, staying updated on trends that could impact company"s network security posture.
- Assisted in the development of security policies and procedures, contributing to organizational compliance initiatives.
- Coordinated network upgrades with minimal disruption to users by scheduling maintenance during off-peak hours.
- Enhanced network security by designing and implementing firewall configurations and policies.
- Contributed to disaster recovery plans, ensuring timely system restoration following unexpected outages.
- Evaluated emerging technologies and recommended suitable

EDUCATION

University of North Texas
Denton, Texas • 04/2018

***Master of Science in Electrical Engineering*:** Electrical Engineering
GPA: 3.92/4.0

K L University
Guntur, Andhra Pradesh • 2016

***Bachelor of Technology*:** Electronics & Communications
GPA: 3.94/4.0

CERTIFICATIONS

- CCNA
- 02/2025 - 02/2028 Cisco
- PCNSE
- 04/2025 - 04/2027 Palo Alto
- Fortinet NSE4
- 03/2025 - 03/2027 Fortinet
- PCNSA
- 01/2025 - 01/2027 Palo Alto

solutions for consideration in future projects or upgrades.

- Designed and implemented VMware NSX micro-segmentation and integrated Palo Alto VM-Series firewalls for secure east-west traffic inspection.
- Managed VMware ESXi/vCenter networking including distributed switches, service insertion, and firewall policy integration.
- Troubleshot connectivity and security issues in virtualized data centers using tools such as vRealize Network Insight (vRNI).
- Administered Palo Alto Next-Gen Firewalls (PA Series & VM-Series) including policy design, migration, and optimization.
- Configured and maintained GlobalProtect VPN, SSL decryption, and advanced security profiles (App-ID, User-ID, Content-ID).
- Performed PAN-OS upgrades, HA configurations, and failover testing to ensure firewall resilience.
- Leveraged Panorama for centralized management, policy push, and device group/template administration.

Bank of America - Network Security Engineer
Dallas, Texas • 11/2023 - 04/2025

- Administered Checkpoint, Fortinet, and Juniper firewalls across BOFA global networks, enhancing security posture and reducing incidents by 6% within 12 months.
- Maintain and document firewall configurations, security policies, and operational procedures, providing knowledge transfer and training to team members.
- Perform end-to-end firewall lifecycle management, including provisioning, policy enforcement, configuration reviews, and decommissioning to maintain a secure network infrastructure.
- Managed and configured all Palo Alto PA 3000 series, PA 5000 series, PA 7000 series firewalls.
- Palo Alto design and installation (VSYS, Application and URL filtering, Threat Prevention, Data Filtering).
- Developed and implemented the Palo Alto hybrid topology by creating IPSEC tunnel from on prem Palo Alto firewall to Virtual Palo Alto in cloud.
- Performed firewall migration from Cisco ASA to Palo Alto firewalls using Palo Alto conversion tool.
- Exposure to wildfire advance malware detection using IPS feature of Palo Alto.
- Support GlobalProtect VPN deployment and maintenance, troubleshooting authentication issues, machine certificate chains, and access control policies.
- Developed and implemented multiple VDOMs and ADOMs on Fortinet firewalls, enhancing network segmentation and improving overall security posture across the organization.
- Utilize tools like Solarwinds, Tufin, Looker, and Tableau to perform network performance analysis and optimize firewall rule sets.
- Worked extensively on deploying Juniper SRX and Net Screen Firewalls and on operational like adding, modifying policies and NAT.
- Assist in access control management, ensuring firewall policies align with business needs while adhering to security best practices.
- Conduct firewall software patching and upgrades, mitigating vulnerabilities while ensuring compliance with security standards and best practices.
- Configure and maintain security policies on Fortinet firewall and managing Fortinet Analyzer.

- Configuring the HA for Checkpoint, Fortinet, Juniper SRX and Net Screen firewalls.
- Working on SIEM Firemon firewall optimization tool and log analysis using IBM Qradar.
- Worked on the Algosec firewall optimization tools to clean up the security policies and remove unused objects from firewalls.
- Configure and manage AWS Network Firewall, Azure Firewall, Web Application Firewall (WAF), and DDoS Protection to safeguard cloud-hosted applications and services.
- Performed Maintenance and backup, system upgrades and restore of Fortinet, Checkpoint, and Juniper Firewall appliances, emergency patch application.
- Deploy and maintain AWS Site-to-Site VPN, Azure VPN Gateway, ExpressRoute, and Direct Connect for secure hybrid and multi-cloud connectivity.
- Working on Implementing the extended ACLs on Juniper SRX to allow communication between the required networks, and to restrict other communications.
- Proactively monitor and analyze firewall logs to detect anomalies, prevent potential threats, and enhance security posture.
- Actively participate in incident response and vulnerability management, investigating security incidents, and implementing mitigation strategies.
- Set up and manage GlobalProtect VPN portals and gateways, enforce security policies, and optimize performance for secure remote access.
- Conducted security policy risk assessments using AlgoSec Security Management Suite, ensuring adherence to security best practices.
- Full-time

Cisco Inc - Network Engineer
Morrisville, NC • 05/2018 - 11/2023

- Maintain and implement all Checkpoint firewall, Cisco ASA firewall and Palo alto change requests from clients. This includes assisting in the correct determination of application flows necessary.
- Provide necessary problem determination in the Checkpoint firewall environment which has Gaia R77.30 Gaia, VSX, Provider-1 and VSX.
- Migration of the firewall rules from Cisco ASA, Checkpoint to Palo Alto firewalls using migration tool from PAN.
- Managed global policy, global groups, and global objects in checkpoint Provider-1/Multi Domain Manager.
- Responsible for firewall rule set migration from Cisco ASA, Checkpoint to newly implemented Palo Alto.
- Configuring HA on checkpoint security gateways using cluster XL and Palo Alto firewalls.
- Streamline VPN operations with Python/Ansible automation, integrate with endpoint security and cloud solutions, and provide user support for seamless access.
- Integrating Panorama with Palo Alto firewalls, managing multiple Palo Alto firewalls using Panorama.
- Palo Alto design and installation (Application and URL filtering, Threat Prevention, Data Filtering).
- Configured and maintained IPSEC and SSL VPNs on Palo Alto Firewalls using Global Protect.
- Deploy and configure GlobalProtect VPN portals and gateways to ensure secure remote access for enterprise users.

- Configure split tunneling and full tunneling policies based on business requirements to optimize network performance and security.
- Firewall rule base review and fine-tuning recommendation using Tufin Secure track.
- Extensive usage of firewall traffic analyzing tools such as tcpdump, snoop, fw monitor, packet captures, and debugs for troubleshooting complex communication problems.
- Collaborate with endpoint security teams to ensure compatibility between GlobalProtect VPN and corporate security solutions such as endpoint protection and device compliance checks.
- Design, implement, and maintain secure network architectures in AWS and Azure, ensuring compliance with security best practices and industry standards.
- Automate VPN deployment and management tasks using scripting languages like Python and Ansible to improve operational efficiency.
- Configured Site to Site IPsec VPN tunnels to peer with different clients and each of client having different specifications of Phase 1 and Phase 2 policies using Cisco ASA 5500 series firewalls.
- Researched, designed, and replaced aging Checkpoint firewall architecture with new next generation Palo Alto appliances serving as firewalls and URL and application inspection.
- Configure Virtual Servers, Nodes, and load balancing Pools in F5 BigIP LTM.
- Provide end-user support and training for VPN connectivity issues, troubleshooting steps, and best practices.
- Configure and manage AWS Security Groups, NACLs, Azure NSGs, and Firewalls to control inbound/outbound traffic and enforce security policies.
- Configure SSL VPN to facilitate various employees access internal servers and resources with access restrictions.
- Used Bluecoat proxy servers for URL and content filtering.
- Using Infoblox IP Address Manager (IPAM) provides a centralized management of the IP address space, including IPv4 and IPv6 Address Management.
- Document test cases, perform operational readiness testing to ensure the networking environment performs as required and document actual results.