Network/Security Administrator

Overview of the role:
Motivated and detail-oriented Network/Security Administrator with over 2–4 years of hands-on experience in configuring, maintaining, and securing enterprise networks. Cisco Certified Network Associate (CCNA) with proven expertise in LAN/WAN infrastructure, firewall policies, VPN deployment, and network monitoring. Adept at identifying vulnerabilities, optimizing network performance, and responding to incidents in compliance with best practices and organizational policies.

Certifications

- Cisco Certified Network Associate (CCNA)
- (Optional) CompTIA Security+ (if multi-certified)
- (Optional) Cisco Certified CyberOps Associate

Skills required

- Cisco routing and switching (IOS configuration, EIGRP, OSPF, VLANs, STP)
- Firewall administration (Cisco ASA, Palo Alto, or Fortinet)
- VPN setup and support (IPSec, SSL)
- Network access control (802.1X, NAC)
- Intrusion detection and prevention systems (IDS/IPS)
- Network monitoring tools (SolarWinds, Nagios, Wireshark)
- Patch management and vulnerability scanning (e.g., Nessus)
- Incident response support and basic forensic analysis
- Basic scripting for automation (Python, Bash)
- Familiar with ITIL or ticketing systems (e.g., ServiceNow)

Typical Responsibilities

- Configure and troubleshoot Cisco routers and switches in enterprise environments
- Maintain network security through access control lists (ACLs), firewall rules, and intrusion prevention systems
- Manage VPN access for remote users and branch offices
- Monitor network traffic and performance to detect anomalies or malicious activity
- Implement routine security patches and firmware updates on network devices

- Collaborate with security teams to support audits and compliance checks
- Respond to and document Tier 1 and Tier 2 security incidents
- Maintain up-to-date network diagrams and documentation

Technical Environment

- Cisco Catalyst and ISR series
- Cisco ASA or Firepower
- Windows Server, Active Directory
- Linux for monitoring/security tools
- Syslog servers, SIEM tools (Splunk, Graylog, or ELK stack)

Soft Skills

- Strong analytical and troubleshooting skills
- Effective communicator with cross-functional teams
- Process-oriented with an eye for documentation
- Continual learner with a strong interest in cybersecurity

Additional information

- Closing date: 31 July 2025
- Type of role: Permanent
- Location: Hybrid Model (Centurion).
- Salary: to be discussed, in line with skills and experience.

This role represents a fantastic opportunity to join a respected team. If you are interested and meet the selection criteria, please send your CV to Keshnee Reddy-Chetty, Keshneer@icetech.io.