We are seeking an experienced **Senior Network & Security Engineer** for one of our clients, a globally recognized enterprise. This role is embedded within a global IT infrastructure organization responsible for designing, optimizing, and maintaining enterprise-grade LAN, WAN, WLAN, and Security environments. You will play a pivotal role in bridging the gap between unique business requirements (including production and R&D facilities) and technical execution—translating needs into High-Level and Low-Level Designs (HLD/LLD) while steering Managed Service Provider (MSP) operations.

Senior Network & Security Engineer

Nr ref.: 246/8/2026/AS/270112/jobs.pl Warszawa (mazowieckie)

What you can expect from us?

- **Long-Term Engagement:** Stable employment under a Contract of Employment (*Umowa o pracę*) aimed at multi-year cooperation.
- **Financial Incentives & Perks:** Annual performance bonus, festive financial rewards, and attractive extra compensation for rotational on-call standby and interventions.
- **Professional Growth:** Full organizational and financial support for continuous learning, including certification exam coverage (Fortinet, Cisco) and a vast offer of internal/external trainings.
- **Hybrid Setup & Comfort:** Hybrid work model (3 days in office / 2 days remote) with flexible working hours and guaranteed free employee parking.
- **Comprehensive Benefits Package:** Premium private medical care (with extension options to family members), life insurance, sports card, language courses, wellbeing initiatives, and meal discounts.

Employment agency entry number 47

this job offer is intended for people over 18 years of age

What will your tasks involve?

- **Architecture & Design:** Translate complex global business requirements into robust High-Level and Low-Level Designs (HLD/LLD) across enterprise LAN, WAN, WLAN, and Security infrastructure.
- **MSP Oversight & L3 Escalations:** Serve as a Subject Matter Expert (SME), guiding the external Managed Service Provider (MSP) in resolving complex Tier-3 incidents, SD-WAN performance issues, and certificate management.
- **Cross-Functional Collaboration:** Act as the critical technical bridge connecting business stakeholders, local facility managers, Cybersecurity teams, and international engineering groups.
- **Process & Agile Optimization:** Operate within an Agile delivery framework to continuously streamline operational workflows, ServiceNow service delivery, and Infrastructure-as-Code (IaC) initiatives.
- **Security Policy Enforcement:** Collaborate with Cybersecurity teams to maintain, tune, and enforce firewall rulesets (Fortinet), Web Application Firewalls (WAF), DNS standards, and secure remote access protocols.

What we expect from you?

- **Extensive Experience:** 5+ years of hands-on experience in large-scale enterprise network and security engineering, with strong expertise in Cisco routing/switching (Catalyst, Nexus) and core protocols (BGP, OSPF, STP, TCP/IP).
- **Firewall & Security Acumen:** Practical experience with enterprise firewalls (preferably Fortinet/FortiGate) and web application security (WAF, SSL inspection, DNS). *Candidates without prior Fortinet experience must be open to completing the Fortinet NSE 4 certification within 6 months (costs fully covered).*
- **Design & Vendor Steering:** Proven track record in creating HLD/LLD documentation and supervising external MSP partners rather than just handling routine L1/L2 operations.
- **Communication & Stakeholder Management:** Exceptional interpersonal skills and fluent English (B2+/C1 mandatory) to drive technical discussions and navigate assertively with international teams across Europe, the US, and Asia.
- **Hybrid & On-Call Availability:** Readiness to work in a hybrid setup (3 days in-office / 2 days remote) and participate in a paid, rotational home standby (On-Call) schedule after onboarding.