Role: Network Security Lead
Area: Business Services
Sub-Area: IT – Cyber & Operations Technology
Location: Dublin / Cork
Salary: Competitive

Duration: Permanent **Ref:** GNI994

Gas Networks Ireland operates and maintains Ireland's €3bn, 14,725km national gas network, which is considered one of the safest and most modern renewables-ready gas networks in the world.

Almost 725,000 Irish homes and businesses trust Ireland's gas network to provide efficient and reliable energy to meet their heating, cooking, manufacturing and transport needs.

The gas network is the cornerstone of Ireland's energy system, securely supplying more than 30% of Ireland's total energy and over 40% of the country's electricity generation.

Gas Networks Ireland is aiming to deliver a repurposed, resized and fully decarbonised gas network by 2045. Its "Pathway to a Net Zero Carbon Network" envisions transforming the existing gas network into two separate systems carrying 100% renewable gas, one dedicated to biomethane and the other to green hydrogen, with the potential to carry approximately 30% biomethane and 70% green hydrogen, as well as offering significant long term energy export opportunities.

Gas Networks is an organisation with a very strong legacy and a culture founded on pride in our purpose, to keep Irelands energy moving, and commitment to our vision, to be at the heart of Irelands energy future. Our organisational values demonstrate what is important across the organisation including building on our experience across our organisation to build towards our sustainable future, doing what's right for each other and for the people and communities that we serve and finally energised for the change of our future towards a renewable energy landscape. Throughout your career in Gas Networks Ireland, you will be part of an organisation that has a strong commitment to supporting and developing our workforce today and into the future. You will also have an opportunity to get involved in our ambitious iBelong programme ensuring a diverse, equitable and inclusive environment for us all to thrive. Finally, our Time to Talk Mental Health programme and our wellbeing initiatives ensure we provide support across many areas as you work in our organisation.

The Role:

Based in Cork or Dublin and reporting to the Cyber Security Manager, this Senior Security Analyst (Network Security Lead) role is central to GNI's mission to strengthen perimeter, edge, and internal segmentation controls, reducing attack surface and enabling secure change at pace. As a senior individual contributor, you will act as the technical lead for firewall architecture, engineering, and operations across on-premises and cloud-connected IT/OT/ET environments - designing policy, assuring high availability and performance, driving secure remote access, and integrating controls with detection/response and vulnerability management. The role follows a hybrid work pattern, requires participation in an

on-call rota, and may involve occasional out-of-hours work. You'll provide day-to-day guidance and performance input for junior analysts, ensuring both operational excellence and knowledge transfer within the team.

Duties and Responsibilities:

1) **Architecture & Design**

- Design and maintain network security architecture (perimeter, DMZ, partner/B2B, data-centre, OT-adjacent), including segmentation and micro-segmentation patterns aligned to Zero Trust principles.
- Define rule base strategy (App-ID/identity-aware policies, service groups, objects, tags) to minimise over-privilege and shadowed/duplicate rules.
- Own NAT, routing interactions (static, dynamic/BGP), and HA/cluster designs ensuring resilience and deterministic failover.
- Plan and govern TLS/SSL decryption policies and privacy exceptions; align with legal and compliance requirements.

2) **Policy Lifecycle & Change Management**

- Run the end-to-end policy lifecycle: intake/impact analysis, risk assessment, change plans and rollbacks, peer review, CAB approvals, and post-implementation validation.
- Lead scheduled rule recertification and hygiene: remove unused, expired, or risky entries; consolidate objects; enforce naming conventions and tagging.
- Maintain golden configs and standard builds; drive PAN-OS / Check Point upgrade roadmaps, including lab validation and staged rollouts.

3) **Operations, Monitoring & Performance**

- Administer and optimise next-gen firewall platforms (e.g., Palo Alto, Check Point) and related proxies/IDPS/PKI/authentication controls.
- Ensure comprehensive logging to SIEM (e.g., Microsoft Sentinel) with high-fidelity alerts and runbooks/SOAR where appropriate.
- Troubleshoot complex flows end-to-end (PCAP/Wireshark, session tables, threat logs, QoS, path MTU, asymmetric routing).
- Maintain and test remote access VPN and site-to-site VPNs; govern posture checks and identity context.
- Ensure regular, tested backups of firewall and network security device configurations; maintain documented restore procedures and participate in periodic recovery drills.
- Plan, schedule, and execute timely patching and firmware updates for all firewall and network security appliances, in line with vendor and organisational SLAs.
- Coordinate and execute vulnerability scans (e.g., Qualys TVM) for firewall and network security infrastructure; track, remediate, and report on vulnerabilities in collaboration with asset owners.
- Continuously monitor firewall and network security health, resource utilisation (CPU, memory, throughput, session counts), and performance metrics; proactively address capacity or degradation issues.

4) **Cloud & Hybrid Connectivity**

- Engineer secure north-south and east-west paths for Azure and other cloud environments (e.g., Azure Firewall, vNGFWs, NSGs/ASGs, Private Link, ExpressRoute).
- Standardise cloud landing-zone security controls and ensure consistent policy across on-prem and cloud.

5) **Security Assurance & Third-Party Oversight**

- Scope and oversee penetration tests/red-team exercises targeting network controls; ensure high-value findings and pragmatic fixes; manage retests to closure.
- Participate in audits; provide accurate evidence of control design and effectiveness.

6) **Incident Response Integration**

- Lead firewall aspects of incident triage/containment (rapid policy updates, network isolation, temporary blocks), contribute to RCA, and convert lessons into durable policy/detections.

7) **Mentorship & Collaboration**

- Provide day-to-day mentorship to junior analysts (design reviews, change walkthroughs, quality gates) while partnering with architects, project teams, and OT stakeholders (e.g., Claroty, DarkTrace) to respect safety/availability constraints.

Knowledge, Skills and Experience:

-
- Degree in Information Systems/IT or equivalent experience; 5+ years IT with 3+ years in network security/firewall engineering (design, build, run).
- Deep hands-on with Palo Alto (PAN-OS, Panorama, App-ID, User-ID, URL/Threat profiles, decryption) and/or Check Point (R8x, SmartConsole/Smart-1, IPS, Identity Awareness).
- Strong grasp of routing/NAT/VPN, HA clustering, BGP/ECMP, DNS, certificates/PKI, and identity-aware policy.
- Experience operating in Azure and hybrid topologies; understanding of cloud networking controls (Azure Firewall, NSGs/ASGs).
- Solid troubleshooting (packet capture, log correlation, path analysis) and SIEM integration (e.g., Microsoft Sentinel).
- Familiarity with automation/IaC (API, Ansible/Terraform) and policy hygiene tooling (e.g., Expedition) is a plus.
- Collaboration and communication skills to explain complex network security topics to technical and non-technical stakeholders; experience mentoring junior team members.

Applications, including current Curriculum Vitae, should be emailed to the following address stating the job title and reference number in the subject line of your email:
recruit@gasnetworks.ie

The closing date for receipt of applications for this vacancy is the 26th of November 2025.

Please note that applications submitted after this closing date will not be accepted.

Gas Networks Ireland is an equal opportunities employer

We are committed to providing a diverse and inclusive place of work and have a robust strategy and framework called ibelong to enable this. We are an equal opportunity employer and through our recruitment process we welcome and encourage applications from interested and suitably qualified individuals regardless of gender, age, racial or ethnic origin, membership of the traveller community, religion or beliefs, family or civil status, sexual orientation/gender identity or disability.

GNI will only hold your data for as long as necessary. By providing a CV to GNI you are agreeing for GNI to process this information about you. If you have any question about how GNI processes your data, please see our Privacy Notice. If you have further questions, you can contact us at DataProtection@gasnetworks.ie