POSITION DESCRIPTION

Specialist Firewall Engineer

POSITION DETAILS

Position Title	Specialist Firewall Engineer
Classification	HEW 7
Position Number	NEW
School/Office	Digital Services / Security & Digital Operations
Division	Division of Operations

POSITION PURPOSE

The Specialist Firewall Engineer plays a critical role in safeguarding the University's digital infrastructure by designing, implementing, and maintaining secure firewall configurations and network security controls. This position ensures the integrity and availability of network services through proactive monitoring, incident response, and continuous improvement of firewall systems. The role also contributes to the strategic uplift of the University's cyber resilience by embedding firewall and network security capabilities into enterprise solutions, supporting audits, and ensuring compliance with internal policies and external standards. The role supports the University's strategic objectives by enabling secure connectivity across research, teaching, and administrative environments.

KEY ACCOUNTABILITIES

- Configure and maintain enterprise firewall systems to ensure secure and reliable network access.
- Monitor firewall performance and security events, responding to incidents and escalating as required.
- Implement firewall rules and policies in alignment with security standards and business requirements.
- Collaborate with IT and Cyber teams to support secure network architecture and segmentation.
- Conduct risk assessments and contribute to firewall-related audits and compliance activities.
- Document firewall configurations, changes, and procedures to support operational continuity.
- Provide technical advice and support to internal stakeholders on firewall-related matters.
- Contribute to continuous improvement initiatives in network security and firewall operations.
- Support capacity planning and lifecycle management for firewall infrastructure to ensure scalability and sustainability.
- Contribute to threat intelligence activities by providing firewall-related insights into attack patterns and vulnerabilities.

QUALIFICATIONS, EXPERIENCE AND SKILLS

- A degree in Cybersecurity, Information Technology, or a related discipline, with at least four years of relevant experience; or an equivalent combination of extensive experience and education/training.
- Demonstrated expertise in firewall technologies, network security protocols, and secure configuration practices.
- Proven ability to independently apply policy and rethink the application of technical knowledge to solve complex problems.
- Experience in interpreting and adapting procedures to meet policy requirements, with impact beyond the immediate work area.
- Strong analytical and diagnostic skills in managing and troubleshooting firewall systems.
- Excellent communication and stakeholder engagement skills, with the ability to provide technical advice and collaborate across teams.
- Experience working in complex hybrid environments spanning on-prem and cloud infrastructures.

Technical Proficiency

- Familiarity with cybersecurity frameworks (e.g., ISO 27001, NIST) and regulatory compliance requirements.
- Proficiency in enterprise firewall technologies (e.g., Palo Alto, Fortinet, Cisco ASA/Firepower, Check Point)
- Strong understanding of network protocols (TCP/IP, BGP, OSPF, VPN, SSL/TLS).
- Familiarity with intrusion detection/prevention systems and SIEM integration.
- Experience with firewall automation, scripting, or Infrastructure-as-Code approaches for configuration management (e.g., Ansible, Terraform).

Desirable

- Experience in higher education or large, federated organisations.
- Exposure to threat intelligence feeds and advanced analytics for firewall event monitoring.
- Relevant vendor certifications (e.g., PCNSE, NSE, CCNP Security).

KEY RELATIONSHIPS

This position reports to: Manager and Cyber Engineer

This position supervises: None

Key internal relationships:

- Cyber Security Assurance and Operations team
- ITDS Infrastructure and Network teams
- Digital Architecture and Governance teams

Key external relationships:

- Firewall and network security vendors
- Sector security forums and partners (e.g., AHECS, AARNET)

CHALLENGES

- Managing complex firewall configurations across hybrid cloud and on-prem environments.
- Responding to evolving threat vectors while maintaining service availability.
- Balancing security requirements with operational and academic needs.
- Ensuring compliance with cybersecurity standards and audit requirements.

OCCUPATION SPECIFIC CAPABILITY SET

SFIA

SFIA Capability	Code	Level	Rationale
Network security	NTAS	5	Designs, configures, and maintains enterprise firewall systems to ensure secure and reliable network access across hybrid environments.
Incident management	USUP	4	Monitors firewall performance and security events; responds to incidents and escalates as required to maintain service availability.
Information security	SCTY	5	Implements firewall rules and policies aligned with security standards and business needs; contributes to risk assessments and compliance activities.
Configuration management	CFMG	4	Maintains accurate documentation of firewall configurations, changes, and procedures to support operational continuity and audit readiness.
Systems integration	SINT	4	Collaborates with IT and Cyber teams to support secure network architecture and segmentation across cloud and on-prem environments.
Stakeholder management	RLMT	4	Provides technical advice and support to internal stakeholders on firewall-related matters, balancing security with operational needs.
Solution architecture	ARCH	4	Contributes to secure network design and continuous improvement initiatives in firewall operations to support strategic objectives.
Capacity management	CPMG	4	Supports capacity planning and lifecycle management of firewall infrastructure to ensure scalability and sustainability.
Threat intelligence	THIN	4	Contributes firewall-specific insights into threat detection, vulnerabilities, and attack patterns to enhance proactive defence.

UNIVERSITY EXPECTATIONS

The University expects that all employees are aware of, and comply with legislation and Western's policies and procedures relevant to the position, including but not limited to:

→ Code of Conduct
→ Work Health and Safety and Wellbeing Management System
→ Enterprise Agreement or Award
→ Anti-discrimination principles, Equal Employment Opportunity and staff and student equity.

Approved by:
Date: