



Australian Government

ICTNWK509 Design and implement a security perimeter for ICT networks

Release: 1

ICTNWK509 Design and implement a security perimeter for ICT networks

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

This unit describes the skills and knowledge required to build a high performance, high security, failure resistant security perimeter, for an enterprise information and communications technology (ICT) network.

It applies to individuals with excellent ICT expertise who are working as middle managers, including information security managers, network engineers, network technicians and security analysts.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Networking

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
1. Plan and design firewall solution	1.1 Determine level and nature of security needed to meet enterprise requirements 1.2 Identify security threats 1.3 Research available perimeter security options 1.4 Design security perimeter to meet identified enterprise requirements
2. Configure perimeter to secure network	2.1 Deploy perimeter devices according to design 2.2 Configure perimeter topology

ELEMENT	PERFORMANCE CRITERIA
	2.3 Configure basic functionality of devices to allow access 2.4 Configure advanced functions
3. Plan, design and configure network devices to provide secure fallover and redundancy	3.1 Back up device configuration 3.2 Design and configure perimeter to enable continuity of service during upgrade of devices 3.3 Design and configure perimeter to enable continuity of service in the event of device failure
4. Plan, design and configure a VPN solution	4.1 Configure perimeter for site-to-site virtual private networks (VPNs) 4.2 Configure perimeter as a remote access VPN server 4.3 Configure perimeter to allow VPN tunnel forwarding 4.4 Diagnose and resolve VPN connectivity issues
5. Test and verify design performance	5.1 Test functionality of basic features 5.2 Test functionality of advanced features 5.3 Perform penetration testing to verify that the perimeter meets security requirements 5.4 Monitor perimeter device performance 5.5 Monitor security breaches 5.6 Document test results and report to appropriate person

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	1.3, 1.4	Gathers, interprets and analyses technical and enterprise information to determine requirements according to client needs
Writing	1.4, 3.2, 3.3, 5.6	Uses factual information and industry related terminology to convey complex technical information, and notes security breaches for client records to clients on technical, operational and business related matters

Oral Communication	1.1, 5.6	• Uses active listening, observational and questioning techniques in order to identify information and confirm, clarify or revise understanding • Reports test results clearly and distinctively, using technical language appropriate to audience and environment
Numeracy	2.3, 2.4, 3.2, 3.3, 4.1-4.3, 5.3	• Selects from and applies an expanding range of mathematical and problem solving strategies to design and configure advanced features of perimeter devices and an integrated VPN solution
Get the work done	1.1, 1.2, 2.1-2.4, 3.1-3.3, 4.1-4.4, 5.1- 5.5	• Reflects on the ways in which digital systems and tools are used or could be used to achieve work goals, and begins to recognise strategic and operational applications • Uses digital technologies and systems safely and securely when implementing and monitoring a system, with a growing awareness of the permanence and transparency of all activities • Uses a combination of formal, logical planning processes and an increasingly intuitive understanding of context to plan, prioritise and monitor own work, and coordinate processes in liaison with others • Makes decisions in relatively complex situations, taking a range of factors into consideration • When dealing with complex issues, may use intuition to identify the general problem area, switching to analytical processes to meet security requirements and resolve other technical problems

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK509 Design and implement a security perimeter for ICT networks	ICANWK509A Design and implement a security perimeter for ICT networks	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTNWK509 Design and implement a security perimeter for ICT networks

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

Evidence of the ability to:

- identify threats to perimeter security
- develop design for a secure perimeter
- deploy perimeter to meet security requirements
- design and configure advanced features of perimeter devices to provide additional services
- design and configure an integrated VPN solution
- conduct exhaustive testing of perimeter.

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- identify and describe emerging security issues and the need for security policies
- describe the security perimeter issues related to networks, including:
 - auditing and penetration testing techniques
 - capabilities of software and hardware perimeter solutions
 - logging analysis techniques
 - organisational network infrastructure
 - security technologies according to perimeter design
 - weaknesses of installed perimeter design.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the network industry, and include access to:

- site or prototype where perimeter security may be implemented and managed
- perimeter devices
- organisational security requirements.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>