



Australian Government

ICTNWK544 Design and implement a security perimeter for ICT networks

Release: 2

ICTNWK544 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 6.0.
Release 2	Correcting an error in Performance Criteria 3.3.

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 advanced ICT expertise and work in roles including middle managers, information security managers, network engineers, network technicians, security analysts or similar.

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 Identify organisational and industry standard security threats according to organisational policies and procedures 1.2 Determine required firewall security according to organisational requirements 1.3 Research and identify available perimeter security options according to organisational requirements 1.4 Design security perimeter according to organisational requirements

ELEMENT	PERFORMANCE CRITERIA
2. Configure perimeter to secure network	2.1 Deploy required perimeter devices according to network security requirements 2.2 Configure required perimeter topology according to network security requirements 2.3 Configure basic functionality of devices according to network security requirements 2.4 Configure required advanced functions according to network security requirements
3. Design and configure network devices	3.1 Back up device configuration according to network security requirements 3.2 Design and configure perimeter and enable continuity of service during devices upgrades 3.3 Design and configure perimeter and enable continuity of service in event of device failure
4. Configure 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 according to network security requirements
5. Test design performance	5.1 Test required functionality of basic features according to network security requirements 5.2 Test required functionality of advanced features according to network security requirements 5.3 Perform required penetration testing and verify perimeter against security requirements 5.4 Document functionality performance results and submit to required personnel

Foundation Skills

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

SKILL	DESCRIPTION
Numeracy	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
Reading	Gathers, interprets and analyses technical and enterprise information

SKILL	DESCRIPTION
	to determine requirements according to client needs
Writing	• 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
Planning and organising	• Uses a combination of formal, logical planning processes to plan, prioritise and monitor own work and coordinate processes in liaison with others and within different contexts
Problem solving	• Makes decisions in relatively complex situations, taking a range of factors into consideration • May use intuition to identify general problem areas from complex issues and switching to analytical processes to meet security requirements and resolve other technical problems
Self-management	• Identifies digital systems and tools are used or could be used to achieve work goals and begins to recognise strategic and operational applications
Technology	• 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

Unit Mapping Information

Supersedes and is equivalent to ICTNWK509 Design and implement a security perimeter for ICT networks.

Links

Companion Volume Implementation Guide is found on VETNet -

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

Assessment Requirements for ICTNWK544 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 6.0.
Release 2	Correcting an error in Performance Criteria 3.3.

Performance Evidence

The candidate must demonstrate the ability to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including evidence of the ability to:

- design, configure and test a security perimeter and integrated VPN solution on network devices on at least one occasion.

In the course of the above, the candidate must:

- design and configure a firewall solution and network devices
- conduct testing of the performance of the perimeter of security devices
- document functionality performance results and the finalised process.

Knowledge Evidence

The candidate must be able to demonstrate knowledge to complete the tasks outlined in the elements, performance criteria and foundation skills of this unit, including knowledge of:

- industry standard emerging security issues and the requirement for security policies
- industry standard security perimeter issues related to networks, including:
 - security technologies according to perimeter design
 - weaknesses of installed perimeter design
- principles and techniques for designing and implementing a security perimeter, including:
 - software and hardware perimeter solutions
 - organisational network infrastructure
 - auditing and penetration testing techniques
 - logging analysis techniques.

Assessment Conditions

Skills in this unit must be demonstrated in a workplace or simulated environment where the conditions are typical of those in a working environment in this industry.

This includes access to:

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

Assessors of this unit must satisfy the requirements for assessors in applicable vocational education and training legislation, frameworks and/or standards.

Links

Companion Volume Implementation Guide is found on VETNet -

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