Australian Government

Department of Education, Employment and Workplace Relations

ICANWK509A Design and implement a security perimeter for ICT networks

Release: 1

ICANWK509A Design and implement a security perimeter for ICT networks

Modification History

Release	Comments
Release 1	This Unit first released with *ICA11 Information and Communications Technology Training Package version 1.0*

Unit Descriptor

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

Application of the Unit

This unit applies to middle managers, such as information security managers, network engineers, network technicians or security analysts, responsible for implementing and managing the organisational network security.

Licensing/Regulatory Information

No licensing, legislative, regulatory or certification requirements apply to this unit at the time of endorsement but users should confirm requirements with the relevant federal, state or territory authority.

Pre-Requisites

Not applicable.

Employability Skills Information

This unit contains employability skills.

Elements and Performance Criteria Pre-Content

Element	Performance Criteria
Elements describe the essential outcomes of a unit of competency.	*Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the required skills and knowledge section and the range statement. Assessment of performance is to be consistent with the evidence guide.*

Elements and Performance Criteria

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*** 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 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

Required Skills and Knowledge

This section describes the skills and knowledge required for this unit.

Required skills

- analytical skills to analyse network information and plan approaches to technical problems or management requirements
- communication skills to:
  - convey and clarify complex information
  - liaise with clients
- literacy skills to interpret and prepare technical documentation, including recording security incidents and developing security policies
- planning skills to plan deployment of the perimeter solution
- problem-solving skills to:
  - design perimeter solution to meet security requirements
  - resolve technical problems
- technical skills to:
  - configure firewalls
  - configure routers
  - deploy perimeter devices to a network
  - test performance of security perimeter to current industry standards.

Required knowledge

- overview knowledge of:
  - emerging security issues
  - emerging security policies
- detailed knowledge of:
  - 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.

Evidence Guide

The evidence guide provides advice on assessment and must be read in conjunction with the performance criteria, required skills and knowledge, range statement and the Assessment Guidelines for the Training Package.

Overview of assessment	
Critical aspects for assessment and evidence required to demonstrate competency in this unit	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.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where perimeter security may be implemented and managed • perimeter devices • organisational security requirements • appropriate learning and assessment support when required. Where applicable, physical resources should include equipment modified for people with special needs.
Method of assessment	A range of assessment methods should be used to assess practical skills and knowledge. The following examples are appropriate for this unit: • verbal or written questioning to assess candidate's knowledge of emerging security issues, security features of hardware and software, limitations in vendor solutions, operating systems and software • direct observation of candidate demonstrating deployment and configuration of a security perimeter • direct observation of candidate conducting testing of secure perimeter • evaluation of report that outlines testing procedures, test results and changes made as a result of testing • evaluation of design and implementation of system in terms of performance and suitability for business needs.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended, where appropriate.

	Assessment processes and techniques must be culturally appropriate, and suitable to the communication skill level, language, literacy and numeracy capacity of the candidate and the work being performed. Indigenous people and other people from a non-English speaking background may need additional support. In cases where practical assessment is used it should be combined with targeted questioning to assess required knowledge.

Range Statement

The range statement relates to the unit of competency as a whole. It allows for different work environments and situations that may affect performance. Bold italicised wording, if used in the performance criteria, is detailed below. Essential operating conditions that may be present with training and assessment (depending on the work situation, needs of the candidate, accessibility of the item, and local industry and regional contexts) may also be included.

Perimeter topology may include:	• 3 legged • back-to-back private • back-to-back public.
Basic functionality may include:	• access control lists (ACLs) • dynamic host configuration protocol (DHCP) • routing • secure network address translation (NAT).
Devices may include:	• Cisco PIX • Cisco router ACLs • ClearOS • Linux iptables • Microsoft ISA Firewall • SmoothWall • Untangle.
Advanced functions may include:	• automated web-client configuration • content filtering • demilitarised zone (DMZ) hosting • firewall policies • forward and reverse caching • load balancing • port forward rules • quality of service (QOS) • server publishing • stateful packet inspection.
VPN tunnel may include:	• IPSec • layer 2 tunnelling protocol (L2TP) • point-to-point tunnelling protocol (PPTP) • secure socket tunnelling protocol (SSTP).

Unit Sector(s)

Networking