Australian Government
Department of Education, Employment and Workplace Relations

ICANWK416A Build security into virtual private networks

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICANWK416A Build security into virtual private 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 security into a virtual private network (VPN).

Application of the Unit

This unit applies to networking staff who are required to ensure that VPNs contain required 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. Configure router to provide for network security monitoring and management	1.1 Create and apply audit rules consistent with ***policies, standards, protocols and management systems*** 1.2 Configure router to provide appropriate level of asset security and monitoring of security consistent with ***commercial and business requirements*** 1.3 Monitor and manage system to assess the level of security and attempts to breach security of ***framework components*** 1.4 Employ appropriate ***hardware*** and ***software*** to monitor and address security issues and provide VPN solutions
2. Secure a site-to-site VPN	2.1 Configure internet key exchange (IKE) and internet protocol security (IPSec) 2.2 Configure site-to-site IPSec VPN using pre-shared keys 2.3 Configure site-to-site IPSec VPN using digital certificates
3. Secure a remote access VPN	3.1 Configure a VPN server 3.2 Install and administer a router-management console 3.3 Develop documentation on current ***system*** settings and framework components and file securely for future reference

Required Skills and Knowledge

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

Required skills

- analytical skills to undertake a network security risk assessment
- initiative and enterprise skills to develop enterprise policies, strategies and procedures
- literacy skills to:
  - interpret audit rules
  - produce security documentation
- numeracy skills to undertake a cost-benefit comparison
- technical skills to:
  - implement LAN, WLAN, VPN and WAN solutions
  - implement security strategies and configure network security software and hardware.

Required knowledge

- characteristics of:
  - auditing and penetration testing techniques
  - configuration of routers and switches
  - security protocols, standards and data encryption
- detailed knowledge of:
  - authentication issues
  - network protocols and operating systems
  - processes and techniques related to security perimeters and their functions
  - security threats, including eavesdropping, data interception, data corruption and data falsification
  - transmission control protocol or internet protocol (TCP/IP) protocols and applications
  - VPNs features, issues and functions
- overview knowledge of:
  - audit and intrusion detection systems
  - LAN, WLAN and WAN
  - organisational issues surrounding security cryptography
  - screened subnets
  - virus detection software.

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: • develop basic security functionality for either VPN, LANs, WANs or WLANs • implement such security • maintain such security • document the security implemented and its maintenance.
Context of and specific resources for assessment	Assessment must ensure access to: • network technical requirements • network infrastructure, including servers and security hardware and software • appropriate learning and assessment support when required • modified equipment 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: • VPNs • WANs • security protocols • review of candidate’s documentation of installed security and its maintenance • evaluation of candidate’s security implementation on a VPN.
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.

Policies may include:	• audit systems • incident response procedures • network intrusion detection systems.
Standards, protocols and management systems may include:	• AAA security • access control lists, context-based control lists • data over cable service interface specification • domain name system security extensions • generic routing encapsulation • IEEE 802.11 Protocol standard for secure wireless local area network products • internet group management protocol • IP security protocol • network port addresses translation (NAT or PAT) • point-to-point network tunnelling protocol • secure: • electronic transactions • multi-purpose internet mail extensions • shell • socket layer and transport layer security.
Commercial and business requirements may include:	• availability • backup • confidentiality • firewalls • hacking prevention • integrity • password logons.
Framework components may include:	• deployment of public key infrastructure (PKI), CA and key management services • firewall technologies • multi-platform directory services supporting relevant standards • operating system capable of providing access control, audit services • support for generalised security services interfaces,

	personnel security • trusted hardware and operating system at selective desktops, servers, network points and mainframes.
Hardware may include:	• desktop and laptop computers, networked and stand-alone • firewall devices • network-monitoring appliances • routers • switches • wired and wireless networks.
Software may include:	• audit • encryption modules • operating system • packaged software but can be supplied from many varying vendors and can include security • virus checking.
System may include:	• applications • databases • external service providers, such as internet service providers (ISPs) and digital certification suppliers • gateways • operating system • servers.

Unit Sector(s)

Networking