Australian Government
Department of Education, Employment and Workplace Relations

ICAB4235B Build basic perimeter security into a network

Release: 1

INDUSTRY SKILLS COUNCILS
Creating Australia's Future

ICAB4235B Build basic perimeter security into a network

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to build basic security into either a virtual private network (VPN), a wireless local area network (WLAN) or local area network (LAN). No licensing, legislative, regulatory or certification requirements apply to this unit at the time of publication.

Application of the Unit

Application of the unit	

Licensing/Regulatory Information

Refer to Unit Descriptor

Pre-Requisites

Prerequisite units		

Employability Skills Information

Employability skills	This unit contains employability skills.

Elements and Performance Criteria Pre-Content

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

ELEMENT	PERFORMANCE CRITERIA
1. Assess vulnerability and threats to system	1.1. Determine levels of required basic perimeter security based on current and future needs of the business 1.2. Assess and report on current system security in line with levels of required security of ***assets*** 1.3. Develop basic security framework and policy if not already present having regard to ***encryption processes***, ***standards***, ***protocols and management systems*** 1.4. Determine ***key network***, ***software***, ***hardware and system*** security performance criteria 1.5. Make recommendations to management to address security deficiencies in line with current and future ***commercial and business requirements***
2. Secure perimeter router	2.1. Configure routers and switches to provide appropriate levels of ***perimeter function*** security 2.2. Disable unneeded services 2.3. Configure supporting security services on related ***network*** services
3. Test and verify performance of security system implemented	3.1. Design test item to verify key measurable performance against criteria 3.2. Conduct tests and record results 3.3. Modify and debug as necessary 3.4. Develop documentation on current system settings and file securely for future reference

Required Skills and Knowledge

REQUIRED SKILLS AND KNOWLEDGE

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

Required skills

- Ability to develop enterprise policies strategies and procedures
- Ability to undertake a network security risk assessment
- Ability to implement security strategies and configure network security software and hardware
- Implementing LAN, WAN, VPN and WLAN solutions

REQUIRED SKILLS AND KNOWLEDGE

- Cost-benefit comparison
- Troubleshooting and debugging

Required knowledge

- Security threats, including eavesdropping, data interception, data corruption, data falsification
- Authentication issues
- Organisational issues surrounding security
- Security perimeters and their functions
- Types of VPNs, including site-to-site, user-to-site internet traffic and extranets
- Function and operation of VPN concepts, including encryption, firewalls, packet tunnelling and authentication
- Common VPN issues, including bandwidth and dynamic security environment
- Network protocols and operating systems
- Security protocols, standards and data encryption
- Configuring routers and switches
- Cryptography
- LAN, WLAN and WAN
- TCP/IP protocols and applications
- Auditing and penetration testing techniques
- Screened subnets
- Virus detection software
- Audit and intrusion detection systems

Evidence Guide

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 following is essential: • Assessment must confirm the ability to develop, implement and maintain basic security functionality for VPNs, LANs, WANs or WLANs To demonstrate competency in this unit the person will require access to: • Network technical requirements • Network infrastructure, including servers and security hardware and software
Context of and specific resources for assessment	The breadth, depth and complexity of knowledge and skills in this competency would cover a broad range of varied activities or application in a wider variety of contexts most of which are complex and non-routine. Leadership and guidance would be involved when organising activities of self and others as well as contributing to technical solutions of a non-routine or contingency nature. Assessment must ensure: • Performance of a broad range of skilled applications including the requirement to evaluate and analyse current practices, develop new criteria and procedures for performing current practices and provision of some leadership and guidance to others in the application and planning of the skills would be characteristic. • Applications may involve responsibility for, and limited organisation of, others.
Method of assessment	The purpose of this unit is to define the standard of performance to be achieved in the workplace. In undertaking training and assessment activities related to

EVIDENCE GUIDE	
	this unit, consideration should be given to the implementation of appropriate diversity and accessibility practices in order to accommodate people who may have special needs. Additional guidance on these and related matters is provided in ICA05 Section 1. • Competency in this unit should be assessed using summative assessment to ensure consistency of performance in a range of contexts. This unit can be assessed either in the workplace or in a simulated environment. However, simulated activities must closely reflect the workplace to enable full demonstration of competency. • Assessment will usually include observation of real or simulated work processes and procedures and/or performance in a project context as well as questioning on underpinning knowledge and skills. The questioning of team members, supervisors, subordinates, peers and clients where appropriate may provide valuable input to the assessment process. The interdependence of units for assessment purposes may vary with the particular project or scenario.
Guidance information for assessment	Holistic assessment with other units relevant to the industry sector, workplace and job role is recommended. An individual demonstrating this competency would be able to: • Demonstrate understanding of a broad knowledge base incorporating some theoretical concepts • Apply solutions to a defined range of unpredictable problems • Identify and apply skill and knowledge areas to a wide variety of contexts, with depth in some areas • Identify, analyse and evaluate information from a variety of sources • Take responsibility for own outputs in relation to specified quality standards • Take limited responsibility for the quantity and quality of the output of others • Maintain knowledge of industry products and

EVIDENCE GUIDE	
	services

Range Statement

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.	
Assets may include:	• data and information • intellectual property • physical assets
Networks may include:	• VPNs • WLANs • WANs
Standards, ***protocols and management systems*** may include:	• IEEE 802.11 Protocol standard for secure wireless local area network products. • AAA security • Secure multi-purpose internet mail extensions • Secure socket layer and transport layer security • IP security protocol • Domain name system security extensions • Data over cable service interface specification • Point-to-point network tunnelling protocol • Secure electronic transactions • Secure shell • Generic routing encapsulation • Network port addresses translation (NAT/PAT) • Access control lists, context-based control lists • Internet group management protocol
Encryption processes may include:	• built-in or third-party products, including sniffers, PKI, SSH, DESlogin, PKZIP, secure socket layer (SSL), digital signatures, Cisco IOS layer encryption, TACACS, RADIUS,

RANGE STATEMENT	
	internet key exchange and simple certificate enrolment protocol
Software may include:	• security • audit • operating systems • virus checking network monitoring software • applications systems • encryption modules
Hardware may include:	• Firewall devices • Routers • Switches • Wired and wireless networks • Network monitoring appliances • Desktop and laptop computers, networked and standalone
Commercial and business requirements	• Back-up and recovery of data • Remote access to internal network • Password logons • Firewalls • Hacking prevention • Confidentiality • Integrity • Availability
System may include:	• databases • applications • servers • operating systems • gateways • application and external agencies, such as ISPs, digital certification providers
Perimeter functions may include:	• identification • authentication • authorisation • access control • auditing • surveillance

Unit Sector(s)

Unit sector	Build

Co-requisite units

Co-requisite units		

Competency field

Competency field	