



Australian Government

Department of Education, Employment and Workplace Relations

ICAB5238B Build a highly secure firewall

Release: 1

ICAB5238B Build a highly secure firewall

Modification History

Not Applicable

Unit Descriptor

Unit descriptor	This unit defines the competency required to build high level security and network functionality into a network by configuring a firewall appropriately. 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. Establish match between firewall appliance and business needs	1.1. Match features and capabilities of firewall appliance to business security needs and asset protection 1.2. Match features and capabilities of firewall appliance to business accounting needs and asset protection 1.3. Match features and capabilities of firewall device to remote access needs and asset protection 1.4. Monitor and manage firewall appliance logs, reports and performance both on-site and remotely
2. Configure firewall appliance	2.1. Configure attack guards and intrusion detection 2.2. Identify and apply IPSec configuration tasks 2.3. Test and verify VPN configuration
3. Secure perimeter using firewall appliance	3.1. Configure appropriate access-defined and access control lists using objects and nested objects as appropriate 3.2. Apply filtering of traffic in line with security requirements 3.3. Configure authentication, authorisation and accounting (AAA) services supporting remote access protocols in line with security requirements 3.4. Document and securely store settings

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, VPN, WLAN and WAN solutions
- Cost-benefit comparison
- Troubleshooting/debugging

Required knowledge

REQUIRED SKILLS AND 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
- The function and operation of virtual private networking (VPN) concepts, including encryption, firewalls, packet tunnelling and authentication
- Common VPN issues, including, bandwidth, dynamic security environment
- Network protocols and operating systems
- Security protocols, standards and data encryption
- Configuring routers and switches
- Cryptography
- LAN, WLAN and WAN solutions
- 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 either VPN, LANs 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 covering planning and initiation of alternative approaches to skills or knowledge applications across a broad range of technical and/or management requirements, evaluation and coordination would be characteristic.

Assessment must ensure:

- The demonstration of competency may also require self-directed application of knowledge and skills, with substantial depth in some areas where judgement is required in planning and selecting appropriate equipment, services and techniques for self and others.
- Applications involve participation in development of strategic initiatives as well as personal responsibility and autonomy in performing complex technical operations or organising others. It may include participation in teams including teams concerned with planning and evaluation functions. Group or team coordination may also be involved.

EVIDENCE GUIDE**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 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 theoretical concepts, with substantial depth in some areas
- Analyse and plan approaches to technical problems or management requirements
- Transfer and apply theoretical concepts and/or technical or creative skills to a range of situations
- Evaluate information, using it to forecast for planning or research purposes

EVIDENCE GUIDE

	• Take responsibility for own outputs in relation to broad quantity and quality parameters • Take some responsibility for the achievement of group outcomes • Maintain knowledge of industry products and 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
<i>Authentication, Authorisation and Accounting (AAA)</i>	• Remote access security approach that controls network access by requiring user identification and restricting access to only particular resources, and maintains records of use for billing and network audit

Unit Sector(s)

Unit sector	Build
--------------------	-------

Co-requisite units

Co-requisite units	

Co-requisite units		

Competency field

Competency field	
-------------------------	--