



Australian Government

Department of Education, Employment and Workplace Relations

ICANWK601A Design and implement a security system

Release: 1

ICANWK601A Design and implement a security system

Modification History

Release	Comments
Release 1	This Unit first released with <i>ICA11 Information and Communications Technology Training Package version 1.0</i>

Unit Descriptor

This unit describes the performance outcomes, skills and knowledge required to use software tools, equipment and protocols to implement a security system.

Application of the Unit

This unit applies to the use of foundational elements of network security, and the description of security threats, securing network devices and their associated networks.

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
<i>Elements describe the essential outcomes of a unit of competency.</i>	<i>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.</i>

Elements and Performance Criteria

1. Assess the security threats facing network Infrastructure	1.1 Evaluate mitigation methods for network attacks and different types of malware 1.2 Propose a methodical concept of defending network architecture
2. Secure edge devices (routers)	2.1 Secure network routers using software tools 2.2 Secure administration access to routers using the router operating system (OS) 2.3 Secure router OS and its configuration file(s)
3. Implement authentication, authorisation and accounting (AAA) and secure access control system (ACS)	3.1 Evaluate and implement the functions and importance of authentication, authorisation and accounting 3.2 Configure the router using AAA 3.3 Analyse and compare the features of TACACS+ and RADIUS AAA protocols for securing the network
4. Mitigate threats to routers and networks using access control lists (ACLs)	4.1 Assess the functionality of access control lists and document the caveats to be considered when building them 4.2 Configure and verify IP ACLs to mitigate threats and to prevent IP address spoofing using tools
5. Implement secure network management and reporting	5.1 Configure secure shell (SSH) on routers to enable secure management 5.2 Configure routers to send log messages to a log server with tools
6. Mitigate common layer 2 attacks	6.1 Document how to prevent layer 2 attacks by configuring basic switch security and features 6.2 Configure switch to prevent layer 2 attacks
7. Implement the router OS firewall-feature set	7.1 Evaluate and compare the operational strategies and weaknesses of the different firewall technologies 7.2 Implement zone-based firewall to strategically secure group of interfaces
8. Implement the intrusion detection and prevention system (IDPS) feature set in the router OS using secure device manager (SDM)	8.1 Evaluate and compare network based versus host based IDPS to identify malicious activity, log information, attempt to block/stop activity, and report activity 8.2 Explain IDPS technologies, attack responses and monitoring options 8.3 Configure the router OS IDPS operations using secure device manager to monitor network and system activities for malicious

	activity
9. Implement site-to-site virtual private networks (VPNs) using SDM	9.1 Assess the different methods used in cryptography 9.2 Evaluate internet key exchange (IKE) protocol functionality and phases to support authentication and define the binding blocks of IPSec and the security functions it provides 9.3 Configure and verify an IPSec site-to-site VPN with pre-shared key (PSK) authentication to provide a secure channel between the two parties

Required Skills and Knowledge

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

Required skills

- communication skills to liaise with internal and external personnel on technical, operational and business-related matters
- literacy skills to:
 - interpret technical documentation
 - write reports as required
- numeracy skills to:
 - take test measurements
 - interpret results
 - evaluate performance and interoperability of network
- planning and organisational skills to:
 - coordinate the process in liaison with others
 - plan, prioritise and monitor own work
- problem-solving and contingency-management skills to:
 - adapt configuration procedures to network requirements
 - reconfigure depending on differing operational contingencies, risk situations and environments
- problem-solving skills to troubleshoot
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
 - select and configure networking devices
 - assess and implement security requirements.

Required knowledge

- access control lists, configuration and troubleshooting
- authentication protocols
- encryption techniques
- IDS and IPS
- IOS and IP networking models and protocols
- current wireless regulations, standards and certifications
- local area network (LAN) or wide area network (WAN) implementations
- malicious attacks and prevention techniques
- network management tools
- network security prevention methods
- procedures to configure, verify and troubleshoot:
 - switch with VLANs and inter-switching communications
 - router
- procedures to set up VPNs
- routing protocols

- threat and attack mitigation techniques
- use of command line interface to configure and test network elements.

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: • evaluate network security system threats and requirements • mitigate attacks and configure firewalls • design and implement network security systems • implement VPN using SDM.
Context of and specific resources for assessment	Assessment must ensure access to: • site where network security may be evaluated and tightened • hardware and software • organisational guidelines, procedures and policies • computers • LAN or WLAN internet work technologies (hardware and software) • security technologies (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: • direct observation of the candidate installing, configuring and testing a new or updated network • evaluation of documentation outlining testing procedures, test results, recommendation to network changes and completion records • verbal or written questioning of required knowledge.
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.

Network may include:	• data • internet • protocol • large and small LANs • virtual LAN (VLAN) • WANs.
Tools may include:	• Cisco security device manager (SDM) • command line interface (CLI) • web interface.
Administration access may include:	• multiple privilege levels • role-based CLI • strong-encrypted passwords.
Features of TACACS+ and RADIUS AAA protocols may include:	• remote authentication dial-in user service (RADIUS): • combines authentication and authorisation • does not allow users to control which commands can be executed on a router • does not support ARA access, NetBIOS Frame Protocol Control Protocol, NASL, and X.25 PAD connections • encrypts only the password in the access-request packet • uses industry standard • uses UDP • TACACS+: • encrypts the entire body of the packet • is Cisco proprietary • offers multiprotocol support • provides two ways to control the authorisation of router commands on a per-user or per-group basis • uses transmission control protocol (TCP) • uses the AAA architecture, which separates authentication, authorisation and accounting.
Access control lists may include:	• extended • named • standard.

Unit Sector(s)

Networking