Australian Government

Department of Education, Employment and Workplace Relations

ICANWK608A Configure network devices for a secure network infrastructure

Release: 1

ICANWK608A Configure network devices for a secure network infrastructure

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 use software tools, equipment and protocols to configure network devices in the design of the infrastructure of a secure network.

Application of the Unit

This unit applies to the use of routers and switches as network elements for a securing networks, and the use of router and switch operating system capabilities to mitigate attacks.

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. Implement layer 2 security	1.1 Configure using router operating system (OS) commands to mitigate layer 2 attacks 1.2 Implement identity-based networking services (IBNS) on switches to provide layer 2 security 1.3 Implement identity management using access control system (ACS) as the authentication server
2. Configure router OS intrusion prevention system (OS-IPS) to mitigate threats to network resources	2.1 Evaluate the advanced capabilities of router OS-IPS firewall feature set to include event action processing (EAP) for ***threats*** to ***network resources*** 2.2 Configure and verify IPS features to identify threats and dynamically block them from entering the network 2.3 Maintain, update and tune the IPS signatures 2.4 Configure and verify context-based access control (CBAC) and network address translation (NAT) to dynamically mitigate identified threats to the network 2.5 Configure and verify zone-based firewall (ZFW) to include advanced application inspections and uniform resource locator (URL) filtering for improved network security
3. Configure virtual private networks (VPNs) to provide secure connectivity for site-to-site and remote access communications	3.1 Analyse and evaluate internet protocol security (IPSec) and generic routing encapsulation (IPSec/GRE) features and functionality 3.2 Configure secure connectivity for site-to-site VPN using certificate authorities 3.3 Analyse dynamic multipoint VPN (DMVPN) features and capabilities 3.4 Configure and verify secure connectivity for site-to-site VPN operations 3.5 Provide highly secure network access with secure socket layer (SSL) VPN to deliver ***remote access connectivity features and benefits*** 3.6 Evaluate ***EasyVPN benefits*** and configure EasyVPN server with dynamic virtual tunnel interface (DVTI) to create a virtual access interface on the virtual tunnel interface 3.7 Configure and verify EasyVPN remote to establish a site-to-site connection using both router and VPN software clients 3.8 Implement group-encrypted transport (GET) VPN features to simplify the provisioning and management of VPN
4. Implement network	4.1 Evaluate NFP features and functionality to provide

foundation protection (NFP)	infrastructure protection 4.2 Secure the management plane, the data plane and the control plane using OS features of the router

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:
  - evaluate performance and interoperability of network
  - interpret results
  - take test measurements
- 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 requirements of network
  - reconfigure depending on differing operational contingencies, risk situations and environments
  - troubleshoot and network security issues
- research skills to investigate appropriate hardware to meet requirements
- technical skills to:
  - assess and implement security requirements
  - select and configure networking devices
  - use networking tools.

Required knowledge

- configuration, verification and troubleshooting procedures to undertake:
  - VLAN switching
  - inter-switching communications
- key features of deployment schemes
- setting up and securing firewalls
- IOS and IP networking models
- local area network (LAN) and wide area network (WAN) implementations
- NAT concepts and configuration
- network topologies, architectures and elements
- networking standards and protocols
- procedures for configuring, verifying and troubleshooting router operations and routing
- secure connectivity and remote access communications
- security protocols, such as SSL
- threat mitigation strategies

- tunnelling protocols
- VPN technologies.

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 requirements • design, implement and verify network security systems using layer 2 and layer 3 devices • mitigate treats to network security • configure VPNs for secure connectivity • evaluate and implement NFP.
Context of and specific resources for assessment	Assessment must ensure access to: • site or prototype where network security may be evaluated and tightened • hardware and software • organisational guidelines, procedures and policies • computers • hardware and software LAN and WLAN internetwork technologies • hardware and software security technologies • 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 prepared by the candidate 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.

Threats may include:	• denial of service (DoS) • IP spoofing • media access control (MAC) spoofing • port scanning • sniffing.
Network resources may include:	• company information • corporate secrets • data • financial data • personal information.
Remote access connectivity features and benefits may include:	• flexible and cost-effective licensing • lower desktop support costs • reduced cost and management complexity • threat protection.
EasyVPN benefits may include:	• deployment flexibility • easy to use and maintain • enhanced interoperability • increased productivity.

Unit Sector(s)

Networking