



Australian Government

ICTNWK608 Configure network devices for a secure network infrastructure

Release: 1

ICTNWK608 Configure network devices for a secure network infrastructure

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Application

This unit describes the 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.

It applies to individuals with advanced information and communications technology (ICT) skills who adapt router and switch operating system capabilities to mitigate attacks.

No licensing, legislative or certification requirements apply to this unit at the time of publication.

Unit Sector

Networking

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
<i>Elements describe the essential outcomes.</i>	<i>Performance criteria describe the performance needed to demonstrate achievement of the element.</i>
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	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

ELEMENT	PERFORMANCE CRITERIA
network resources	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 foundation protection (NFP)	4.1 Evaluate NFP features and functionality to provide infrastructure protection 4.2 Secure the management plane, the data plane and the control plane using OS features of the router

Foundation Skills

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Performance Criteria	Description
Reading	2.1, 2.2, 3.1, 3.3, 3.6, 4.1	- Organises, evaluates and critiques ideas and information from a range of complex texts - Draws on a broad range of strategies to build and maintain understanding throughout complex texts
Writing	1.1-1.3, 2.2-2.5, 3.2, 3.4, 3.6, 3.7	- Generates complex written texts, demonstrating control over a broad range of writing styles and purposes - Writes and edits computer code and technical data ensuring correct syntax and accuracy
Numeracy	2.2, 2.4, 2.5, 3.4, 3.7	Selects from, and flexibly applies, a wide range of highly developed mathematical and problem solving strategies and techniques in a broad range of contexts
Get the work done	1.1, 1.2, 1.3, 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 4.1, 4.2	- Plans strategic priorities and outcomes within a flexible, efficient and effective context in a diverse environment exposed to competing demands - Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and understand the uses and potential of new technology - Uses a broad range of strategies to store, access and organise virtual information recognising that design choices will influence what information is retrieved and how it may be interpreted and used - Explores and incubates new and innovative ideas through unconstrained analysis and critical thinking

Unit Mapping Information

Code and title current version	Code and title previous version	Comments	Equivalence status
ICTNWK608 Configure network devices for a secure network infrastructure	ICANWK608A Configure network devices for a secure network infrastructure	Updated to meet Standards for Training Packages	Equivalent unit

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>

Assessment Requirements for ICTNWK608 Configure network devices for a secure network infrastructure

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 1.0.

Performance Evidence

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 threats to network security
- configure virtual private networks (VPNs) for secure connectivity
- evaluate and implement network foundation protection (NFP).

Note: If a specific volume or frequency is not stated, then evidence must be provided at least once.

Knowledge Evidence

To complete the unit requirements safely and effectively, the individual must:

- explain configuration, verification and troubleshooting procedures to undertake:
 - virtual local area network (VLAN) switching
 - inter-switching communications
- outline the key features of deployment schemes
- summarise setting up and securing firewalls
- explain iDevice operating system (iOS) and internet protocol (IP) networking models
- outline local area network (LAN) and wide area network (WAN) implementations
- explain network address translation (NAT) concepts and configuration
- outline network topologies, architectures and elements
- explain networking standards and protocols
- outline procedures for configuring, verifying and troubleshooting router operations and routing
- summarise secure connectivity and remote access communications
- explain security protocols, such as secure socket layer (SSL)
- clarify threat mitigation strategies

- outline tunnelling protocols
- summarise VPN technologies.

Assessment Conditions

Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the networking industry, and include access to:

- a 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.

Assessors must satisfy NVR/AQTF assessor requirements

Links

Companion Volume implementation guides are found in VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2>