



Australian Government

Assessment Requirements for ICTNWK609 Configure and manage intrusion prevention system on network sensors

Release: 1

Assessment Requirements for ICTNWK609 Configure and manage intrusion prevention system on network sensors

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 intrusion prevention system (IPS) requirements and configure IPS sensors
- tune up IPS sensors to optimise attack mitigation
- use network tools and network management tools to monitor and manage security sensor events
- upgrade and maintain IPS sensors.

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 a switch and router operation and routing protocol
- outline deployment schemes
- summarise setting up and securing firewalls
- summarise internetwork operating system (IOS) and internet protocol (IP) networking models
- explain IP addressing and detailed understanding of the transmission control protocol (TCP) or IP stack
- outline IPS and intrusion detection system (IDS) strategies
- explain IPS sensor technologies and licensing requirements
- outline local area network or wide area network (LAN/WAN) implementations and design
- summarise network topologies, architectures and elements
- outline networking standards and protocols
- explain signatures and meta signatures
- explain threat mitigation strategies

- explain virtual local area network (VLAN) concepts and functionality
- outline virtual private network (VPN) technologies
- identify and describe legislation, regulations, standards and codes of practice relevant to network security.

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 installation may be conducted
- relevant hardware and software
- organisational guidelines
- live network
- an IPS system and its sensors.

Assessors must satisfy NVR/AQTF assessor requirements.

Links

Companion Volume implementation guides are found in VETNet -

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