Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

FEBRUARY 2013

CONSUMER GUIDE: CISCO UNIFIED WIRELESS NETWORK (CUWN)

Product Description

1. The Cisco Unified Wireless Network (CUWN) provides end-to-end wireless encryption, centralised WLAN management, Authentication, Authorisation and Accounting (AAA) and WLAN policy enforcement. The CUWN comprises multiple wireless products, including the Cisco Wireless Access Points (WAP) and Wireless LAN Controllers (WLC).

Evaluation Scope

2. The scope of the DCE included the following functionality;

   - Authentication
   - Data Confidentiality
   - Data Integrity

3. The Wireless Intrusion Prevention System (WIPS) component of the CUWN was deemed out of scope for the purpose of the DCE, as the WIPS does not include any cryptographic functionality.

DSD’s Findings

4. DSD performed a cryptographic evaluation on the product in addition to the Common Criteria (CC) evaluation.

5. As the product has successfully completed a DCE, it can be used to downgrade the requirements of PROTECTED data in transit to those of UNCLASSIFIED, in accordance with the Australian Government Information Security Manual (ISM).

6. When choosing wireless products, agencies should be aware that the security of any WPA2 Enterprise wireless network is dependant on each of the network components and how they interact with each other. WPA2 Enterprise wireless networks typically comprise of three main elements:

   - Supplicant software: software that supports the 802.1X protocol, and is therefore able to authenticate to a wireless Access Point (AP) or Ethernet switch.

- Wireless LAN Controllers and Wireless Access Points: devices that relay data between the supplicant software and the RADIUS server.
- RADIUS servers: back-end management servers used for authentication, authorisation and accounting purposes.

DSD's Recommendations

7. Agencies using CUWN as part of a PROTECTED wireless network MUST adhere to the following recommendations;

   7.1. The CISCO WLAN product must be used in conjunction with supplicant software that has successfully completed a DCE.

   7.2. Devices running supplicant software take on the classification of the network they are connected to and MUST be protected accordingly.

   7.3. The WLC-to-RADIUS connection MUST be either:

   i) Provided via a wired link that has been accredited to communicate data classified at the same level of the wireless network, or

   ii) Be encapsulated with an additional layer of encryption (on top of the RADIUS encapsulation). *Note: if this option is used, network encryption products (e.g. IPSec or SSL VPN products) that have successfully completed a DCE MUST be used to provide the additional layer of encryption*.

   7.4. Agencies MUST use WPA2 in Enterprise mode.

   7.5. Agencies MUST use AES-CCMP for data confidentiality and integrity.

   7.6. Mutual authentication MUST be performed via EAP-TLS with X.509 certificates for both supplicant and WLC authentication.

   7.7. Unique certificates SHOULD be used for both devices and users accessing a wireless network.

   7.8. Agencies MUST use a Public Key Infrastructure (PKI) product or Hardware Security Module (HSM) that as completed a DCE to generate X.509 certificates.

   7.9. Certificates used to grant access to a classified network take on the classification of the network and MUST be protected accordingly.

8. Agencies using CUWN as part of an UNCLASSIFIED wireless network SHOULD refer to the Wireless Local Area Network section within the ISM.

9. Recommendations given in this Consumer Guide take precedence over those in the ISM where there is a conflict.

Contact Details

10. For further information regarding the certification of these products, or compliance with the ISM, please contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian Government Information Security Manual

11. The advice given in this document is in accordance with the *Australian Government Information Security Manual*, release date September 2012.

Date of this Consumer Guide

12. This Consumer Guide was issued by DSD on 19 February 2013.