

Wireless Network Security

Security Features Checklist

Core Security Functionality

Encryption - support WPA2 encryption
 Identity Protection
 Denial of Service Attack
 Replay Attack
 On-line Dictionary Attack
 Waiting Period
 Off-line Dictionary Attack
 Man-in-the-Middle Attack
 Disable Promiscuous Mode

Conformance to Protocol Standards

IEEE 802.11 - Select from 802.11a, 802.11g or 802.11n
 802.11i - Wi-Fi Protected Access 2
 Disable Wired Equivalent Privacy
 Disable Wi-Fi Protected Access

Authentication

802.1x - should support this protocol.
 Mutual Authentication

PKI Standards

Compatible with existing infrastructure

Cryptographic Standards

Encryption Algorithms

Advanced Encryption Standard (AES)
 Triple- Data Encryption Standard (3DES)

Key Establishment Algorithms

Rivest, Shamir, Adleman (RSA)
 Other algorithms based on exponentiation of finite fields
 Key Exchange Algorithm (KEA)
 Elliptic Curve algorithms

Digital Signature Algorithms

RSA
 Digital Signature Algorithm (DSA)
 Other algorithms based on exponentiation of finite fields
 Elliptic Curve Digital Signature Algorithm (ECDSA)

Hashing Algorithms

SHA-1
 SHA-224
 SHA-256
 SHA-384
 SHA-512

Cryptoperiod

Should be appropriate for the algorithm in use

Assurance Standards

FIPS 140-1
 FIPS 140-2
 Common Criteria (CC) Evaluation Assurance Level (EAL) 3 or higher
 Protection Profile or Security Target

Configurability

Hide SSID
 Change default SSID

Usability

Configuration by Users
 Authentication by Users
 Maintenance by Administrators
 Reconfiguration by Administrators

Manageability

Authentication of Management Traffic
 Central Management
 Encryption of Management Traffic

Scalability

Roaming features
 Support for multiple access points
 Authentication of Management Traffic
 Central Management
 Encryption of Management Traffic