# Mapping Between

# Network Device Collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, May 29, 2015

# and

# NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **AC-18.** The primary purpose of a WLAN Access System is to facilitate wireless connectivity to an organizational network, in support of AC-18. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that those are all implemented in support of ensuring the proper implementation of AC-18.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or EP supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to limit connectivity based on usage conditions such as day/time restrictions only supports AC-2(11) to the extent that the TOE can enforce usage conditions on access to a wireless network; it cannot enforce usage conditions on services that are outside of its own boundary.
- **Extended Package.** A TOE that conforms to this extended package will also conform to the collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. This extended package refines some of the NDcPP requirements to ensure consistency between the PP and the package, but this does not affect the security controls that satisfying those requirements is intended to address.

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| **TOE Security Functional Requirements** | | | | |
| FCS_CKM.1(2) | **Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)** | SC-12 | **Cryptographic Key Establishment and Management** | The ability of the TOE to generate symmetric keys satisfies the key generation portion of this control. |
| | | SC-12(2) | **Cryptographic Key Establishment and Management:** Symmetric Keys | A conformant TOE ensures that generated symmetric keys provide an appropriate level of security. |
| FCS_CKM.2(2) | **Cryptographic Key Distribution (PMK)** | SC-12 | **Cryptographic Key Establishment and Management** | A conformant TOE's implementation of this function supports the key distribution portion of this control. |
| FCS_CKM.2(3) | **Cryptographic Key Distribution (GTK)** | SC-12 | **Cryptographic Key Establishment and Management** | A conformant TOE's implementation of this function supports the key distribution portion of this control. |
| FIA_AFL.1 | **Authentication Failure Handling** | AC-7 | **Unsuccessful Logon Attempts** | The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occurs and take some corrective action. |
| FIA_UAU.6 | **Re-authenticating** | IA-11 | **Re-Authentication** | A conformant TOE supports this control by enforcing re-authentication of the administrator when certain conditions are met. |
| FIA_8021X_EXT.1 | **Extended: 802.1X Port Access Entity (Authenticator) Authentication** | IA-3 | **Device Identification and Authentication** | A conformant TOE supports this control by enforcing 802.1X as a mechanism to perform device authentication. |
| FIA_PSK_EXT.1 | **Extended: Pre-Shared Key Composition** | IA-5 | **Authenticator Management** | A conformant TOE uses pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (g) of the control. |
| FPT_FLS.1 | **Failure with preservation of secure state** | SC-24 | **Fail in Known State** | A conformant TOE supports this control by ensuring that a secure state is maintained in the event of a failure. |

| Common Criteria Version 3.x SFR | | NIST SP 800-53 Revision 5 Control Supports | | Comments and Observations |
|---|---|---|---|---|
| FTA_TSE.1 | **TOE Session Establishment** | AC-2(11) | **Account Management:** Usage Conditions | A conformant TOE supports this control by preventing the establishment of wireless sessions unless configured usage conditions are met. |
| **Optional Requirements** | | | | |
| FPT_ITT.1 | **Basic Internal TSF Data Transfer Protection** | SC-8 | **Transmission Confidentiality and Integrity** | A conformant TOE supports this control by implementing a mechanism to protect the confidentiality and integrity of data in transit between TOE components. |
| | | SC-8(1) | **Transmission Confidentiality and Integrity:** Cryptographic Protection | A conformant TOE supports this control by using a cryptographic mechanism to protect data in transit between distributed components. |
| FCS_CKM.2(4) | **Cryptographic Key Distribution** | SC-12 | **Cryptographic Key Establishment and Management** | A conformant TOE's implementation of this function supports the key distribution portion of this control. |
| **Selection-Based Requirements** | | | | |
| This EP has no selection-based requirements. | | | | |
| **Objective Requirements** | | | | |
| This EP has no objective requirements. | | | | |