DataSoft RAP-117 Security Target

Version 1.4
07/25/2023

Prepared for:

DataSoft Corporation

10235 S. 51st Street, Suite 115
Phoenix, AZ 85044

Prepared By:

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is RAP-117 provided by DataSoft Corporation. The TOE is being evaluated as a network device.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – DataSoft RAP-117 Security Target

ST Version – Version 1.4

ST Date – 07/25/2023

1.2 TOE Reference

TOE Identification – DataSoft RAP-117

TOE Developer – DataSoft Corporation

Evaluation Sponsor – DataSoft Corporation

1.3 TOE Overview

The Target of Evaluation (TOE) is the Datasoft RAP-117 (HW version 2.0 and FW version 2.2.0).

1.4 TOE Description

The TOE provides a small form factor Radio Access Point (RAP), which allows mobile and dismounted operators to perform Command and Control (or "C2") related computing functions securely across existing tactical communications networks. With the ability to process the data communications for a variety of C2-related applications, the TOE is a lightweight subsystem that provides Wi-Fi connectivity (with support for multicast traffic) between commercial mobile computing platforms (i.e., smartphone, tablet, etc.) and the secure military radios (through the TOE's Ethernet radio connection) at the tactical edge.

1.4.1 TOE Architecture

An administrator uses a dedicated provisioning application (running on the administrator's workstation) to administer the TOE. The NDcPP terms the dedicated provisioning application as a "Management Component" and because the TOE independently satisfies all SFRs in the cPP (as well as the SFRs of the PP Modules) without the Management Component, the NDcPP22e prescribes that the TOE be certified (by itself) according to the cPP and without the Management Component. "Figure 4: Non-distributed TOE use case" in the NDcPP22e depicts the TOE and its dedicated provisioning applications.

As a result, the TOE boundary includes only the TOE itself, and the dedicated provisioning application (along with the administrator's workstation upon which the application runs) lies in the TOE's Operational Environment.

1.4.1.1 Physical Boundaries

The RAP-117 includes three physical interfaces, 802.11 wireless, Ethernet, and USB-to-Ethernet. The RAP-117 includes Wi-Fi radio hardware and access point software to support its wireless personal area network (PAN) interface. The RAP includes software to route traffic between its PAN interface and its Ethernet interface, which the TOE uses to communicate with the tactical radio.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the RAP-117:

- Security audit
- Cryptographic support
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

1.4.1.2.1 Security audit

The TOE provides auditing capabilities to provide a secure and reliable way to trace all changes to the system. Any administrative configuration changes during provisioning and other auditable events are audited internally and then transmitted externally over a secure communication channel to an audit server. All audited events have the necessary details like timestamp, event log, event code, and identity of the party involved to provide a comprehensive audit trail.

1.4.1.2.2 Cryptographic support

The TOE provides cryptographic functions for secure administration access via SSH; for communications with VPN clients via IPsec; for wireless communication via WPA2/WPA3 and for communication to external systems such as

audit log servers and RADIUS via IPsec. Functions include Key generation, key establishment, key distribution, key destruction, and cryptographic operations.

1.4.1.2.3 Identification and authentication

The TOE provides secure connectivity between wireless clients via 802.1X authentication. The TOE supports certificate based authentication via external RADIUS server and supports SAE authentication via a local authentication mechanism. The TOE provides secure password-based and pubkey based authentication for remote administrators. The TOE also provides strong password requirements that the administrator can configure, including length, session timeout and password complexity. Consecutive unsuccessful attempts beyond a certain limit will result in locking of the user for a specified duration of time or until user unlock by another administrator.

1.4.1.2.4 Security management

TOE administrators manage the security functions of the TOE through a SSH CLI. Administration cannot be performed from a wireless client. The TOE also provides the ability to configure the session activity timeout of an administrator and to configure the TOE's access banner.

1.4.1.2.5 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established with trusted VPN peers and VPN Clients. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

1.4.1.2.6 Protection of the TSF

The TOE provides image integrity verification to validate the authenticity of the images before loading them. Upon every boot up, power on self-tests are conducted to validate the integrity of the software components. If power-up self-tests fail, the TOE halts boot. The TOE also allows manual configuration of the TOE's real time clock (RTC) by administrators. The TOE protects cryptographic keys and passwords from unauthorized access.

1.4.1.2.7 TOE access

The TOE offers a login banner which provides the administrator to ability to display a custom warning/access policy message as per the organization needs. The TOE is capable of restricting wireless access based on time and day. The TOE provides the ability to configure an inactivity timeout which terminates the session beyond the inactivity period configured. An administrator can also terminate their own session.

1.4.1.2.8 Trusted path/channels

The TOE communicates to external components in a secure manner using WPA2/WPA3 for wireless clients and using IPsec for VPN Clients, a RADIUS server, and a syslog server. The TOE also employs SSH to secure remote administrative sessions.

1.4.2 TOE Documentation

Datasoft Common Criteria Guide for the RAP-117, July 25, 2023 (Admin Guide)

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Conformant
- PP-Configuration for Network Devices, VPN Gateways, and Wireless Local Area Network (WLAN) Access System, Version 1.0 (CFG_NDcPP-VPNGW-WLANAS_V1.0), which includes the following components:
    - Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
    - PP-Module: PP-Module for VPN Gateways, Version 1.2 (MOD_VPNGW_V1.2)
    - PP-Module: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLAN_AS_V1.0)
- Technical Decisions:

Package	Technical Decision	Applied	Rationale for exclusion
CPP_ND_V2.2E	TD0738 - NIT Technical Decision for Link to Allowed-With List	Yes	
MOD_VPNGW_v1.2	TD0723 – Correction to ECDSA Curve Selection	Yes	
MOD_VPNGW_v1.2	TD0683 – RFC 2460 to be replace with RFC 8200	Yes	
MOD_WLAN_AS_v1.0	TD0680 - OS 4.2.1 Conformance Claims section updated to allow for MOD_WLAN_CLI_v1.0	Yes	Not directly applicable as the TOE is a WLAN AS not a client.
MOD_WLAN_AS_v1.0	TD0679 - Handling Standalone WLANAS TOEs with Single Interfaces	Yes	
CPP_ND_V2.2E	TD0670 - NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	No	TLS not claimed.
MOD_VPNGW_v1.2	TD0657 - IPSEC_EXT.1.6 GCM support for VPN GW	Yes	
MOD_VPNGW_v1.2	TD0656 - Missing EAs for VPN GW Optional Headend SFRs	Yes	
MOD_WLAN_AS_v1.0	TD0651 - WLAN AS as Distributed and Non-distributed TOE	Yes	
CPP_ND_V2.2E	TD0639 - NIT Technical Decision for Clarification for NTP MAC Keys	No	NTP not claimed.
CPP_ND_V2.2E	TD0638 - NIT Technical Decision for Key Pair Generation for Authentication	Yes	
CPP_ND_V2.2E	TD0636 - NIT Technical Decision for Clarification of Public Key User Authentication for SSH	Yes	
CPP_ND_V2.2E	TD0635 - NIT Technical Decision for TLS Server and Key Agreement Parameters	No	TLS not claimed.
CPP_ND_V2.2E	TD0634 - NIT Technical Decision for Clarification required for testing IPv6	Yes	

Package	Technical Decision	Applied	Rationale for exclusion
CPP_ND_V2.2E	TD0633 - NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	Yes	
CPP_ND_V2.2E	TD0632 - NIT Technical Decision for Consistency with Time Data for vNDs	Yes	The TD modifies the possible selections; however, as the TOE is not a vND, the selection introduced by the TD is not utilized.
CPP_ND_V2.2E	TD0631 - NIT Technical Decision for Clarification of public key authentication for SSH Server	Yes	
CPP_ND_V2.2E	TD0592 - NIT Technical Decision for Local Storage of Audit Records	Yes	
CPP_ND_V2.2E	TD0591 - NIT Technical Decision for Virtual TOEs and hypervisors	Yes	
CPP_ND_V2.2E	TD0581 - NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	Yes	
CPP_ND_V2.2E	TD0580 - NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	Yes	
CPP_ND_V2.2E	TD0572 - NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	Yes	
CPP_ND_V2.2E	TD0571 - NiT Technical Decision for Guidance on how to handle FIA_AFL.1	Yes	
CPP_ND_V2.2E	TD0570 - NiT Technical Decision for Clarification about FIA_AFL.1	Yes	
CPP_ND_V2.2E	TD0569 - NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	No	DTLSS not claimed.
CPP_ND_V2.2E	TD0564 - NiT Technical Decision for Vulnerability Analysis Search Criteria	Yes	
CPP_ND_V2.2E	TD0563 - NiT Technical Decision for Clarification of audit date information	Yes	
CPP_ND_V2.2E	TD0556 - NIT Technical Decision for RFC 5077 question	Yes	
CPP_ND_V2.2E	TD0555 - NIT Technical Decision for RFC Reference incorrect in TLSS Test	No	TLSS not claimed.
CPP_ND_V2.2E	TD0547 - NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	Yes	
CPP_ND_V2.2E	TD0546 - NIT Technical Decision for DTLS - clarification of Application Note 63	No	DTLS not claimed.
CPP_ND_V2.2E	TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	TLSC not claimed.
CPP_ND_V2.2E	TD0536 - NIT Technical Decision for Update Verification Inconsistency	Yes	
CPP_ND_V2.2E	TD0528 - NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	No	NTP not claimed.
CPP_ND_V2.2E	TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	

2.1 Conformance Rationale

The ST conforms to the set of protection profiles described in section 2 above (and abbreviated as NDcPP22e/VPNGW12/WLANAS10). As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the NDcPP22e/VPNGW12/WLANAS10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e/VPNGW12/WLANAS10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e/VPNGW12/WLANAS10 should be consulted if there is interest in that material.

In general, the NDcPP22e/VPNGW12/WLANAS10 has defined Security Objectives appropriate for network devices and as such are applicable to the RAP-117 TOE.

3.1 Security Objectives for the Operational Environment

OE.ADMIN_CREDENTIALS_SECURE The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.CONNECTIONS See TD0520 for SARs.
The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.RESIDUAL_INFORMATION The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

OE.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.
For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e/VPNGW12/WLANAS10. The NDcPP22e/VPNGW12/WLANAS10 defines the following extended requirements and since they are not redefined in this ST the NDcPP22e/VPNGW12/WLANAS10 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0633
- VPNGW12:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0657
- WLANAS10:FCS_IPSEC_EXT.1: IPsec Protocol
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
- WLANAS10:FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
- VPNGW12:FIA_X509_EXT.2: X.509 Certificate Authentication
- NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
- WLANAS10:FMT_SMR_EXT.1: No Administration from Client
- VPNGW12:FPF_RUL_EXT.1: Packet Filtering Rules
- NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
- NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
- NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
- NDcPP22e:FPT_TST_EXT.1: TSF testing
- VPNGW12:FPT_TST_EXT.1: TSF Testing
- WLANAS10:FPT_TST_EXT.1: TSF Testing
- VPNGW12:FPT_TST_EXT.3: Self-Test with Defined Methods
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- VPNGW12:FPT_TUD_EXT.1: Trusted Update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
- VPNGW12:FTA_VCM_EXT.1: VPN Client Management - per TD0656

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the NDcPP22e/VPNGW12/WLANAS10. The refinements and operations already performed in the NDcPP22e/VPNGW12/WLANAS10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e/VPNGW12/WLANAS10 and any residual operations have been completed herein. Of particular note, the NDcPP22e/VPNGW12/WLANAS10 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the NDcPP22e/VPNGW12/WLANAS10. The NDcPP22e/VPNGW12/WLANAS10 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by RAP-117 TOE.

Requirement Class	Requirement Component
FAU: Security audit	NDcPP22e:FAU_GEN.1: Audit Data Generation
	VPNGW12:FAU_GEN.1/VPN: Audit Data Generation (VPN Gateway)
	WLANAS10:FAU_GEN.1/WLAN: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation
	VPNGW12:FCS_CKM.1/IKE: Cryptographic Key Generation (for IKE Peer Authentication)
	WLANAS10:FCS_CKM.1/WPA: Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	NDcPP22e:FCS_CKM.2: Cryptographic Key Establishment
	WLANAS10:FCS_CKM.2/GTK: Cryptographic Key Distribution (GTK)
	WLANAS10:FCS_CKM.2/PMK: Cryptographic Key Distribution (PMK)
	NDcPP22e:FCS_CKM.4: Cryptographic Key Destruction
	NDcPP22e:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	VPNGW12:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	WLANAS10:FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)
	NDcPP22e:FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)
	NDcPP22e:FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)
	NDcPP22e:FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)
	NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0633
	VPNGW12:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0657
	WLANAS10:FCS_IPSEC_EXT.1: IPsec Protocol
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
FIA: Identification and authentication	WLANAS10:FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication
	NDcPP22e:FIA_AFL.1: Authentication Failure Management
	NDcPP22e:FIA_PMG_EXT.1: Password Management

	WLANAS10:FIA_UAU.6: Re-Authenticating
	NDcPP22e:FIA_UAU.7: Protected Authentication Feedback
	NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
	NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	VPNGW12:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	NDcPP22e:FMT_MOF.1/Functions: Management of Security Functions Behaviour
	NDcPP22e:FMT_MOF.1/ManualUpdate: Management of security functions behaviour
	NDcPP22e:FMT_MTD.1/CoreData: Management of TSF Data
	NDcPP22e:FMT_MTD.1/CryptoKeys: Management of TSF Data
	VPNGW12:FMT_MTD.1/CryptoKeys: Management of TSF Data
	NDcPP22e:FMT_SMF.1: Specification of Management Functions - per TD0631
	WLANAS10:FMT_SMF.1/AccessSystem: Specification of Management Functions (WLAN Access Systems)
	VPNGW12:FMT_SMF.1/VPN: Specification of Management Functions
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles
	WLANAS10:FMT_SMR_EXT.1: No Administration from Client
FPF: Packet Filtering	VPNGW12:FPF_RUL_EXT.1: Packet Filtering Rules
FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	WLANAS10:FPT_FLS.1: Failure with Preservation of Secure State
	VPNGW12:FPT_FLS.1/SelfTest: Failure with Preservation of Secure State (Self-Test Failures)
	NDcPP22e:FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	NDcPP22e:FPT_STM_EXT.1: Reliable Time Stamps - per TD0632
	NDcPP22e:FPT_TST_EXT.1: TSF testing
	VPNGW12:FPT_TST_EXT.1: TSF Testing
	WLANAS10:FPT_TST_EXT.1: TSF Testing
	VPNGW12:FPT_TST_EXT.3: Self-Test with Defined Methods
	NDcPP22e:FPT_TUD_EXT.1: Trusted update
	VPNGW12:FPT_TUD_EXT.1: Trusted Update
FTA: TOE access	NDcPP22e:FTA_SSL.3: TSF-initiated Termination
	NDcPP22e:FTA_SSL.4: User-initiated Termination
	NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking
	NDcPP22e:FTA_TAB.1: Default TOE Access Banners
	WLANAS10:FTA_TSE.1: TOE Session Establishment
	VPNGW12:FTA_VCM_EXT.1: VPN Client Management - per TD0656
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel - per TD0639
	WLANAS10:FTP_ITC.1: Inter-TSF Trusted Channel
	WLANAS10:FTP_ITC.1/Client: Inter-TSF Trusted Channel (WLAN Client Communications)
	VPNGW12:FTP_ITC.1/VPN: Inter-TSF Trusted Channel (VPN Communications)
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path - per TD0639

Table 1 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Audit Data Generation (NDcPP22e:FAU_GEN.1)

NDcPP22e:FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
- Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- Resetting passwords (name of related user account shall be logged).
- [***no other actions***];
d) Specifically defined auditable events listed in Table 2.

NDcPP22e:FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of **Table 2**.

Requirement	Audit Event	Additional Contents
NDcPP22e:FAU_GEN.1		
VPNGW12:FAU_GEN.1/VPN		
WLANAS10:FAU_GEN.1/WLAN		
NDcPP22e:FAU_GEN.2		
NDcPP22e:FAU_STG.1		
NDcPP22e:FAU_STG_EXT.1		
NDcPP22e:FCS_CKM.1		
VPNGW12:FCS_CKM.1/IKE		
WLANAS10:FCS_CKM.1/WPA		
NDcPP22e:FCS_CKM.2		
WLANAS10:FCS_CKM.2/GTK		
WLANAS10:FCS_CKM.2/PMK		
NDcPP22e:FCS_CKM.4		
NDcPP22e:FCS_COP.1/DataEncryption		
NDcPP22e:FCS_COP.1/Hash		
NDcPP22e:FCS_COP.1/KeyedHash		
NDcPP22e:FCS_COP.1/SigGen		
VPNGW12:FCS_EAP_EXT.1		
NDcPP22e:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
WLANAS10:FCS_IPSEC_EXT.1/WLAN	Protocol failures. Establishment or Termination of an IPsec SA.	Reason for failure. Non-TOE endpoint of connection. Non-TOE endpoint of connection.
NDcPP22e:FCS_RBG_EXT.1		
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
WLANAS10:FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to	Provided client identity (e.g. Media Access Control [Media

Requirement	Audit Event	Additional Contents
	successful completion of the authentication exchange. Failed authentication attempt.	Access Control (MAC)] address). Provided client identity (e.g. MAC address).
NDcPP22e:FIA_AFL.1	Unsuccessful login attempt limit is met or exceeded.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_PMG_EXT.1		
WLANAS10:FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UAU.7		
NDcPP22e:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
NDcPP22e:FIA_X509_EXT.2		
VPNGW12:FIA_X509_EXT.2		
NDcPP22e:FIA_X509_EXT.3		
NDcPP22e:FMT_MOF.1/Functions		
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	
NDcPP22e:FMT_MTD.1/CoreData		
NDcPP22e:FMT_MTD.1/CryptoKeys		
VPNGW12:FMT_MTD.1/CryptoKeys		
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	
WLANAS10:FMT_SMF.1/AccessSystem		
VPNGW12:FMT_SMF.1/VPN	All administrative actions.	
NDcPP22e:FMT_SMR.2		
WLANAS10:FMT_SMR_EXT.1		
VPNGW12:FPF_MFA_EXT.1		
VPNGW12:FPF_RUL_EXT.1	Application of rules configured with the 'log' operation.	Source and destination addresses Source and destination ports Transport Layer Protocol.
NDcPP22e:FPT_APW_EXT.1		
WLANAS10:FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
VPNGW12:FPT_FLS.1/SelfTest		
NDcPP22e:FPT_SKP_EXT.1		
NDcPP22e:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
NDcPP22e:FPT_TST_EXT.1		

Requirement	Audit Event	Additional Contents
VPNGW12:FPT_TST_EXT.1		
WLANAS10:FPT_TST_EXT.1	Execution of TSF self-test. Detected integrity violations.	None. The TSF code file that caused the integrity violation.
VPNGW12:FPT_TST_EXT.3		
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	
VPNGW12:FPT_TUD_EXT.1		
NDcPP22e:FPT_TUD_EXT.2	Failure of update.	Reason for failure (including identifier of invalid certificate).
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	
NDcPP22e:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	
NDcPP22e:FTA_TAB.1		
WLANAS10:FTA_TSE.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
VPNGW12:FTA_VCM_EXT.1		
NDcPP22e:FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
WLANAS10:FTP_ITC.1	Failed attempts to establish a trusted channel (including IEEE 802.11). Detection of modification of channel data.	Identification of the initiator and target of channel.
WLANAS10:FTP_ITC.1/Client		
VPNGW12:FTP_ITC.1/VPN	Initiation of the trusted channel Termination of the trusted channel Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channel establishment attempt.
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	

Table 2 Audit Events

5.1.1.2 Audit Data Generation (VPN Gateway) (VPNGW12:FAU_GEN.1/VPN)

VPNGW12:FAU_GEN.1.1/VPN

The TSF shall be able to generate an audit record of the following auditable events:
a. Start-up and shutdown of the audit functions
b. Indication that TSF self-test was completed
c. Failure of self-test
d. All auditable events for the not specified level of audit; and
e. auditable events defined in the Auditable Events for Mandatory Requirements table.

VPNGW12:FAU_GEN.1.2/VPN

The TSF shall record within each audit record at least the following information:
a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, additional information defined in the Auditable Events for Mandatory Requirements table for each auditable event, where applicable.

5.1.1.3 Audit Data Generation (WLANAS10:FAU_GEN.1/WLAN)

WLANAS10:FAU_GEN.1.1/WLAN

The TSF shall be able to generate an audit record of the following auditable events:
a. Start-up and shutdown of the audit functions;
b. All auditable events for the not specified level of audit; and
c. Auditable events listed in the Auditable Events table (Table 2)
d. Failure of wireless sensor communication

5.1.1.4 User identity association (NDcPP22e:FAU_GEN.2)

NDcPP22e:FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.1.1.5 Protected Audit Event Storage (NDcPP22e:FAU_STG_EXT.1)

NDcPP22e:FAU_STG_EXT.1.1

The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

NDcPP22e:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition
[***The TOE shall consist of a single standalone component that stores audit data locally,***]

NDcPP22e:FAU_STG_EXT.1.3

The TSF shall [***overwrite previous audit records according to the following rule: [overwriting the oldest previous audit records]***] when the local storage space for audit data is full.

5.1.2 Cryptographic support (FCS)

5.1.2.1 Cryptographic Key Generation (NDcPP22e:FCS_CKM.1)

NDcPP22e:FCS_CKM.1.1

The TSF shall generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm: [
- ECC schemes using 'NIST curves' [P-256, P-384] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]].

5.1.2.2 Cryptographic Key Generation (for IKE Peer Authentication) (VPNGW12:FCS_CKM.1/IKE)

VPNGW12:FCS_CKM.1.1/IKE

The TSF shall generate asymmetric cryptographic keys used for IKE peer authentication in accordance with a specified cryptographic key generation algorithm:
[***- FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4 for ECDSA schemes and implementing 'NIST curves' P-384 and [no other curves]***]
and
[***- no other key generation algorithm***]
and specified cryptographic key sizes [*equivalent to, or greater than, a symmetric key strength of 112 bits*]. (TD0723 applied)

5.1.2.3 Cryptographic Key Generation (Symmetric Keys for WPA2 Connections) (WLANAS10:FCS_CKM.1/WPA)

WLANAS10:FCS_CKM.1.1/WPA

The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [*PRF-384 and [**PRF512, PRF-704**]*] and specified cryptographic key sizes [*256 bits and [**128 bits**]*] using a Random Bit Generator as specified in FCS_RBG_EXT.1 that meet the following: [*IEEE 802.11-2020 and [**IEEE 802.11ax-2021**]*].

5.1.2.4 Cryptographic Key Establishment (NDcPP22e:FCS_CKM.2)

NDcPP22e:FCS_CKM.2.1

The TSF shall perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography' (TD0581 applied),
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526] (TD0580 applied)].

5.1.2.5 Cryptographic Key Distribution (GTK) (WLANAS10:FCS_CKM.2/GTK)

WLANAS10:FCS_CKM.2.1/GTK

The TSF shall distribute GTK in accordance with a specified cryptographic key distribution method: [***AES Key Wrap in an EAPOL-Key frame***] that meets the following: [*NIST SP 800-38F, IEEE 802.11-2020 for the packet format and timing considerations*] and does not expose the cryptographic keys.

5.1.2.6 Cryptographic Key Distribution (PMK) (WLANAS10:FCS_CKM.2/PMK)

WLANAS10:FCS_CKM.2.1/PMK

The TSF shall receive the 802.11 PMK in accordance with a specified cryptographic key distribution method: [*from 802.1X Authorization Server*] that meets the following: [*IEEE 802.11-2020*] and does not expose the cryptographic keys.

5.1.2.7 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4)

NDcPP22e:FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method
- For plaintext keys in volatile storage, the destruction shall be executed by a [***single overwrite consisting of [zeroes]***];
- For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [***logically addresses the storage location of the key***

and performs a [[four]-pass] overwrite consisting of [a pseudo-random pattern using the TSF's RBG, zeroes], instructs a part of the TSF to destroy the abstraction that represents the key] that meets the following: No Standard.

5.1.2.8 Cryptographic Operation (AES Data Encryption/Decryption) (NDcPP22e:FCS_COP.1/DataEncryption)

NDcPP22e:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***GCM***] mode and cryptographic key sizes [***256 bits***] that meet the following: AES as specified in ISO 18033-3, [***GCM as specified in ISO 19772***].

5.1.2.9 Cryptographic Operation (AES Data Encryption/Decryption) (VPNGW12:FCS_COP.1/DataEncryption)

VPNGW12:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, GCM***] and [***no other***] mode and cryptographic key sizes [***256 bits***], and [***no other cryptographic key sizes***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, GCM as specified in ISO 19772***] and [***no other standards***].

5.1.2.10 Cryptographic Operation (AES Data Encryption/Decryption) (WLANAS10:FCS_COP.1/DataEncryption)

WLANAS10:FCS_COP.1.1/DataEncryption

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm Advanced Encryption Standard (AES) used in Cipher Block Chaining (CBC), CCM mode Protocol (CCMP), and [***GCMP***] modes and cryptographic key sizes 256 bits and [***128 bits***] that meet the following: AES as specified in ISO 18033-3, CBC as specified in ISO 10116, CCMP as specified in NIST SP 800-38C and IEEE 802.11-2020, [***GCMP as specified in NIST SP 800-38D and IEEE 802.11ax-2021***].

5.1.2.11 Cryptographic Operation (Hash Algorithm) (NDcPP22e:FCS_COP.1/Hash)

NDcPP22e:FCS_COP.1.1/Hash

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384, SHA-512***] and message digest sizes [***256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

5.1.2.12 Cryptographic Operation (Keyed Hash Algorithm) (NDcPP22e:FCS_COP.1/KeyedHash)

NDcPP22e:FCS_COP.1.1/KeyedHash

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-384***] and cryptographic key sizes [**384**] and message digest sizes [***384***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

5.1.2.13 Cryptographic Operation (Signature Generation and Verification) (NDcPP22e:FCS_COP.1/SigGen)

NDcPP22e:FCS_COP.1.1/SigGen

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [384 bits]]
that meet the following:
- For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-384]; ISO/IEC 14888-3, Section 6.4].

5.1.2.14 IPsec Protocol - per TD0633 (NDcPP22e:FCS_IPSEC_EXT.1)

NDcPP22e:FCS_IPSEC_EXT.1.1
The TSF shall implement the IPsec architecture as specified in RFC 4301.

NDcPP22e:FCS_IPSEC_EXT.1.2
The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

NDcPP22e:FCS_IPSEC_EXT.1.3
The TSF shall implement [***tunnel mode***].

NDcPP22e:FCS_IPSEC_EXT.1.4
The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [***AES-CBC-256 (specified in RFC 3602), AES-GCM-256 (RFC 4106)***] together with a Secure Hash Algorithm (SHA)-based HMAC [***HMAC-SHA-384***].

NDcPP22e:FCS_IPSEC_EXT.1.5
The TSF shall implement the protocol: [***- IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23], and [RFC 4868 for hash functions]***].

NDcPP22e:FCS_IPSEC_EXT.1.6
The TSF shall ensure the encrypted payload in the [***IKEv2***] protocol uses the cryptographic algorithms [***AES-CBC-256 (specified in RFC 3602), AES-GCM-256 (specified in RFC 5282)***].

NDcPP22e:FCS_IPSEC_EXT.1.7
The TSF shall ensure that [***- IKEv2 SA lifetimes can be configured by a Security Administrator based on [o length of time, where the time values can be configured within [3-24] hours]***].

NDcPP22e:FCS_IPSEC_EXT.1.8
The TSF shall ensure that [***- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [o length of time, where the time values can be configured within [1-8] hours]***].

NDcPP22e:FCS_IPSEC_EXT.1.9
The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [**256 or greater**] bits.

NDcPP22e:FCS_IPSEC_EXT.1.10
The TSF shall generate nonces used in [***IKEv2***] exchanges of length [***- according to the security strength associated with the negotiated Diffie-Hellman group***].

NDcPP22e:FCS_IPSEC_EXT.1.11
The TSF shall ensure that IKE protocols implement DH Group(s) [***[19 (256-bit Random ECP), 20 (384-bit Random ECP) according to RFC 5114]***].

NDcPP22e:FCS_IPSEC_EXT.1.12
The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 IKE_SA***] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 CHILD_SA***] connection.

NDcPP22e:FCS_IPSEC_EXT.1.13
The TSF shall ensure that all IKE protocols perform peer authentication using [***ECDSA***] that use X.509v3 certificates that conform to RFC 4945 and [***no other method***].

NDcPP22e:FCS_IPSEC_EXT.1.14
The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: [***SAN: IP address***] and [***no other reference identifier type***].

5.1.2.15 IPsec Protocol - per TD0657 (VPNGW12:FCS_IPSEC_EXT.1)

VPNGW12:FCS_IPSEC_EXT.1.1
The TSF shall implement the IPsec architecture as specified in RFC 4301.

VPNGW12:FCS_IPSEC_EXT.1.2
The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

VPNGW12:FCS_IPSEC_EXT.1.3
The TSF shall implement [***tunnel mode***].

VPNGW12:FCS_IPSEC_EXT.1.4
The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [***AES-CBC-256 (specified in RFC 3602), AES-GCM-256 (specified in RFC 4106)***] and [***no other algorithm***] together with a Secure Hash Algorithm (SHA)-based HMAC [***HMAC-SHA-384***].

VPNGW12:FCS_IPSEC_EXT.1.5
The TSF shall implement the protocol: [***IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23] and [RFC 4868 for hash functions]***].

VPNGW12:FCS_IPSEC_EXT.1.6
The TSF shall ensure the encrypted payload in the [***IKEv2***] protocol uses the cryptographic algorithms [***AES-CBC-256 (specified in RFC 3602), AES-GCM-256 (specified in RFC 5282)***]. (TD0657 applied)

VPNGW12:FCS_IPSEC_EXT.1.7
The TSF shall ensure that [***IKEv2 SA lifetimes can be configured by a Security Administrator based on [length of time, where the time values can be configured within [3-24] hours]***].

VPNGW12:FCS_IPSEC_EXT.1.8
The TSF shall ensure that [***IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [length of time, where the time values can be configured within [1-8] hours]***].

VPNGW12:FCS_IPSEC_EXT.1.9
The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ('x' in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [**256 or greater**] bits.

VPNGW12:FCS_IPSEC_EXT.1.10
The TSF shall generate nonces used in [***IKEv2***] exchanges of length [***according to the security strength associated with the negotiated DH group, at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash***].

VPNGW12:FCS_IPSEC_EXT.1.11
The TSF shall ensure that IKE protocols implement DH Group(s)
- 19 (256-bit Random ECP), 20 (384-bit Random ECP) according to RFC 5114 and
- [***[no other DH Groups] according to RFC 5114***].

VPNGW12:FCS_IPSEC_EXT.1.12
The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 IKE_SA***] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [***IKEv2 CHILD_SA***] connection.

VPNGW12:FCS_IPSEC_EXT.1.13
The TSF shall ensure that all IKE protocols perform peer authentication using [***ECDSA***] that use X.509v3 certificates that conform to RFC 4945 and [***no other method***].

VPNGW12:FCS_IPSEC_EXT.1.14
The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: Distinguished Name (DN), [***no other reference identifier type***].

5.1.2.16 Random Bit Generation (NDcPP22e:FCS_RBG_EXT.1)

NDcPP22e:FCS_RBG_EXT.1.1
The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [***CTR_DRBG (AES)***].

NDcPP22e:FCS_RBG_EXT.1.2
The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[one] platform-based noise source***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011Table C.1 'Security Strength Table for Hash Functions', of the keys and hashes that it will generate.

5.1.2.17 SSH Server Protocol - per TD0631 (NDcPP22e:FCS_SSHS_EXT.1)

NDcPP22e:FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol that complies with: RFC(s) 4251, 4252, 4253, 4254, [***4256, 4344, 5647, 5656, 6668, 8268, 8308 section 3.1, 8332***].
NDcPP22e:FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following user authentication methods as described in RFC 4252: public key-based, [***password-based***].
NDcPP22e:FCS_SSHS_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**263,144**] bytes in an SSH transport connection are dropped.
NDcPP22e:FCS_SSHS_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes256-gcm@openssh.com***].
NDcPP22e:FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [***ecdsa-sha2-nistp384***] as its public key algorithm(s) and rejects all other public key algorithms.
NDcPP22e:FCS_SSHS_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [***implicit***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).
NDcPP22e:FCS_SSHS_EXT.1.7
The TSF shall ensure that [***ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384***] are the only allowed key exchange methods used for the SSH protocol.
NDcPP22e:FCS_SSHS_EXT.1.8
The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.1.3 Identification and authentication (FIA)

5.1.3.1 802.1X Port Access Entity (Authenticator) Authentication (WLANAS10:FIA_8021X_EXT.1)

WLANAS10:FIA_8021X_EXT.1.1
The TSF shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the 'Authenticator' role.
WLANAS10:FIA_8021X_EXT.1.2
The TSF shall support communications to a RADIUS authentication server conforming to RFCs 2865 and 3579.
WLANAS10:FIA_8021X_EXT.1.3
The TSF shall ensure that no access to its 802.1X controlled port is given to the wireless client prior to successful completion of this authentication exchange.

5.1.3.2 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within [**3-10**] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

NDcPP22e:FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met, the TSF shall [***prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [an unlock action] is taken by an Administrator***
prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.1.3.3 Password Management (NDcPP22e:FIA_PMG_EXT.1)

NDcPP22e:FIA_PMG_EXT.1.1

The TSF shall provide the following password management capabilities for administrative passwords:
a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: : [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')', /= + - _ ` ~ |] [{ } ~ ' ; : / ? . > , <***/] ;
b) Minimum password length shall be configurable to between [**6**] and [**16**] characters.

5.1.3.4 Re-Authenticating (WLANAS10:FIA_UAU.6)

WLANAS10:FIA_UAU.6.1

The TSF shall re-authenticate the administrative user under the conditions [*when the user changes their password, [**no other conditions**]*].

5.1.3.5 Protected Authentication Feedback (NDcPP22e:FIA_UAU.7)

NDcPP22e:FIA_UAU.7.1

The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.

5.1.3.6 Password-based Authentication Mechanism (NDcPP22e:FIA_UAU_EXT.2)

NDcPP22e:FIA_UAU_EXT.2.1

The TSF shall provide a local [***password-based, SSH public key-based***] authentication mechanism to perform local administrative user authentication.

5.1.3.7 User Identification and Authentication (NDcPP22e:FIA_UIA_EXT.1)

NDcPP22e:FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:
- Display the warning banner in accordance with FTA_TAB.1;
- [***no other actions***].

NDcPP22e:FIA_UIA_EXT.1.2

The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.1.3.8 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/Rev)

NDcPP22e:FIA_X509_EXT.1.1/Rev

The TSF shall validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

- The TSF shall validate the revocation status of the certificate using [***Certificate Revocation List (CRL) as specified in RFC 5759 Section 5***]
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
  - o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

NDcPP22e:FIA_X509_EXT.1.2/Rev

The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.9 X.509 Certificate Authentication (NDcPP22e:FIA_X509_EXT.2)

NDcPP22e:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***IPsec***], and [***no additional uses***].

NDcPP22e:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.10 X.509 Certificate Authentication (VPNGW12:FIA_X509_EXT.2)

VPNGW12:FIA_X509_EXT.2.1

The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec and [***no other protocols***], and [***no additional uses***].

VPNGW12:FIA_X509_EXT.2.2

When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [***not accept the certificate***].

5.1.3.11 X.509 Certificate Requests (NDcPP22e:FIA_X509_EXT.3)

NDcPP22e:FIA_X509_EXT.3.1

The TSF shall generate a Certification Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [***device-specific information, Common Name***].

NDcPP22e:FIA_X509_EXT.3.2

The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.4 Security management (FMT)

5.1.4.1 Management of Security Functions Behaviour (NDcPP22e:FMT_MOF.1/Functions)

NDcPP22e:FMT_MOF.1.1/Functions

The TSF shall restrict the ability to [***modify the behaviour of***] the functions [***transmission of audit data to an external IT entity***] to Security Administrators.

5.1.4.2 Management of security functions behaviour (NDcPP22e:FMT_MOF.1/ManualUpdate)

NDcPP22e:FMT_MOF.1.1/ManualUpdate

The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

5.1.4.3 Management of TSF Data (NDcPP22e:FMT_MTD.1/CoreData)

NDcPP22e:FMT_MTD.1.1/CoreData

The TSF shall restrict the ability to manage the TSF data to Security Administrators.

5.1.4.4 Management of TSF Data (NDcPP22e:FMT_MTD.1/CryptoKeys)

NDcPP22e:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.4.5 Management of TSF Data (VPNGW12:FMT_MTD.1/CryptoKeys)

VPNGW12:FMT_MTD.1.1/CryptoKeys

The TSF shall restrict the ability to manage the cryptographic keys and certificates used for VPN operation to Security Administrators.

5.1.4.6 Specification of Management Functions - per TD0631 (NDcPP22e:FMT_SMF.1)

NDcPP22e:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions:
- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [***digital signature***] capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [***Ability to modify the behavior of the transmission of audit data to an external IT entity,***
Ability to manage the cryptographic keys,
Ability to configure the cryptographic functionality,
Ability to configure the lifetime for IPsec SAs,
Ability to re-enable an Administrator account,
Ability to set the time which is used for time-stamps;
Ability to configure the reference identifier for the peer;
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors,
Ability to import X509v3 certificates to the TOE's trust store,
Ability to manage the trusted public keys database].

5.1.4.7 Specification of Management Functions (WLAN Access Systems) (WLANAS10:FMT_SMF.1/AccessSystem)

WLANAS10:FMT_SMF.1.1/AccessSystem

The TSF shall be capable of performing the following management functions:
- Configure the security policy for each wireless network, including:
- Security type
- Authentication protocol
- Client credentials to be used for authentication
- Service Set Identifier (SSID)
- If the SSID is broadcasted
- Frequency band set to [***2.4 GHz, 5 GHz***]
- Transmit power level

5.1.4.8 Specification of Management Functions (VPNGW12:FMT_SMF.1/VPN)

VPNGW12:FMT_SMF.1.1/VPN

The TSF shall be capable of performing the following management functions:
- Definition of packet filtering rules;
- Association of packet filtering rules to network interfaces;

- Ordering of packet filtering rules by priority;
- [***No other capabilities***].

5.1.4.9 Restrictions on Security Roles (NDcPP22e:FMT_SMR.2)

NDcPP22e:FMT_SMR.2.1
The TSF shall maintain the roles: - Security Administrator.
NDcPP22e:FMT_SMR.2.2
The TSF shall be able to associate users with roles.
NDcPP22e:FMT_SMR.2.3
The TSF shall ensure that the conditions
- The Security Administrator role shall be able to administer the TOE locally;
- The Security Administrator role shall be able to administer the TOE remotely
are satisfied.

5.1.4.10 No Administration from Client (WLANAS10:FMT_SMR_EXT.1)

WLANAS10:FMT_SMR_EXT.1.1
The TSF shall ensure that the ability to administer remotely the TOE from a wireless client shall be disabled by default.

5.1.5 Packet Filtering (FPF)

5.1.5.1 Packet Filtering Rules (VPNGW12:FPF_RUL_EXT.1)

VPNGW12:FPF_RUL_EXT.1.1
The TSF shall perform Packet Filtering on network packets processed by the TOE.
VPNGW12:FPF_RUL_EXT.1.2
The TSF shall allow the definition of Packet Filtering rules using the following network protocols and protocol fields:
- IPv4 (RFC 791)
  - o source address
  - o destination address
  - o protocol
- IPv6 (RFC 2460)
  - o source address
  - o destination address
  - o next Header (protocol)
- TCP (RFC 793)
  - o source port
  - o destination port
- UDP (RFC 768)
  - o source port
  - o destination port.

VPNGW12:FPF_RUL_EXT.1.3
The TSF shall allow the following operations to be associated with Packet Filtering rules: permit and drop with the capability to log the operation.
VPNGW12:FPF_RUL_EXT.1.4
The TSF shall allow the Packet Filtering rules to be assigned to each distinct network interface.
VPNGW12:FPF_RUL_EXT.1.5
The TSF shall process the applicable Packet Filtering rules (as determined in accordance with VPNGW12:FPF_RUL_EXT.1.4) in the following order: Administrator-defined.
VPNGW12:FPF_RUL_EXT.1.6
The TSF shall drop traffic if a matching rule is not identified.

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Protection of Administrator Passwords (NDcPP22e:FPT_APW_EXT.1)

NDcPP22e:FPT_APW_EXT.1.1
The TSF shall store administrative passwords in non-plaintext form.
NDcPP22e:FPT_APW_EXT.1.2
The TSF shall prevent the reading of plaintext administrative passwords.

5.1.6.2 Failure with Preservation of Secure State (WLANAS10:FPT_FLS.1)

WLANAS10:FPT_FLS.1.1
The TSF shall preserve a secure state when the following types of failures occur: failure of the self-tests.

5.1.6.3 Failure with Preservation of Secure State (Self-Test Failures) (VPNGW12:FPT_FLS.1/SelfTest)

VPNGW12:FPT_FLS.1.1/SelfTest
The TSF shall shut down when the following types of failures occur: failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.

5.1.6.4 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) (NDcPP22e:FPT_SKP_EXT.1)

NDcPP22e:FPT_SKP_EXT.1.1
The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.1.6.5 Reliable Time Stamps - per TD0632 (NDcPP22e:FPT_STM_EXT.1)

NDcPP22e:FPT_STM_EXT.1.1
The TSF shall be able to provide reliable time stamps for its own use.
NDcPP22e:FPT_STM_EXT.1.2
The TSF shall [***allow the Security Administrator to set the time***].

5.1.6.6 TSF testing (NDcPP22e:FPT_TST_EXT.1)

NDcPP22e:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [***during initial start-up (on power on)***] to demonstrate the correct operation of the TSF: [**integrity check of TOE executable code and cryptographic algorithm self-tests**].

5.1.6.7 TSF Testing (VPNGW12:FPT_TST_EXT.1)

VPNGW12:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [***during initial startup (on power on)***] to demonstrate the correct operation of the TSF: noise source health tests, [**integrity check of TOE executable code and cryptographic algorithm self-tests**].

5.1.6.8 TSF Testing (WLANAS10:FPT_TST_EXT.1)

WLANAS10:FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests during initial start-up (on power on) and [***in no other circumstances***] to demonstrate the correct operation of the TSF: integrity verification of stored TSF executable code when it is loaded for execution through the use of the TSF-provided cryptographic service specified in FCS_COP.1/SigGen, [***[cryptographic algorithm self-tests]***].

5.1.6.9 Self-Test with Defined Methods (VPNGW12:FPT_TST_EXT.3)

VPNGW12:FPT_TST_EXT.3.1
The TSF shall run a suite of the following self-tests when loaded for execution to demonstrate the correct operation of the TSF: integrity verification of stored executable code.

VPNGW12:FPT_TST_EXT.3.2
The TSF shall execute the self-testing through a TSF-provided cryptographic service specified in FCS_COP.1/SigGen.

5.1.6.10 Trusted update (NDcPP22e:FPT_TUD_EXT.1)

NDcPP22e:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

NDcPP22e:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

NDcPP22e:FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a [***digital signature***] prior to installing those updates.

5.1.6.11 Trusted Update (VPNGW12:FPT_TUD_EXT.1)

VPNGW12:FPT_TUD_EXT.1.1
The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [***no other TOE firmware/software version***].

VPNGW12:FPT_TUD_EXT.1.2
The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [***no other update mechanism***].

VPNGW12:FPT_TUD_EXT.1.3
The TSF shall provide means to authenticate firmware/software updates to the TOE using a digital signature mechanism and [***no other mechanisms***] prior to installing those updates.

5.1.7 TOE access (FTA)

5.1.7.1 TSF-initiated Termination (NDcPP22e:FTA_SSL.3)

NDcPP22e:FTA_SSL.3.1
The TSF shall terminate a remote interactive session after a Security Administrator-configurable time interval of session inactivity.

5.1.7.2 User-initiated Termination (NDcPP22e:FTA_SSL.4)

NDcPP22e:FTA_SSL.4.1
The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.1.7.3 TSF-initiated Session Locking (NDcPP22e:FTA_SSL_EXT.1)

NDcPP22e:FTA_SSL_EXT.1.1
The TSF shall, for local interactive sessions, [***terminate the session***] after a Security Administrator-specified time period of inactivity.

5.1.7.4 Default TOE Access Banners (NDcPP22e:FTA_TAB.1)

NDcPP22e:FTA_TAB.1.1

Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

5.1.7.5 TOE Session Establishment (WLANAS10:FTA_TSE.1)

WLANAS10:FTA_TSE.1.1

The TSF shall be able to deny session establishment of a wireless client session based on TOE interface, time, day, [***no other attributes***].

5.1.7.6 VPN Client Management - per TD0656 (VPNGW12:FTA_VCM_EXT.1)

VPNGW12:FTA_VCM_EXT.1.1

The TSF shall assign a private IP address to a VPN client upon successful establishment of a security session.

5.1.8 Trusted path/channels (FTP)

5.1.8.1 Inter-TSF trusted channel - per TD0639 (NDcPP22e:FTP_ITC.1)

NDcPP22e:FTP_ITC.1.1

The TSF shall be capable of using [***IPsec***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [***[802.1X authentication server]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

NDcPP22e:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

NDcPP22e:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**syslog-ipsec communications, radius-ipsec communications**].

5.1.8.2 Inter-TSF Trusted Channel (WLANAS10:FTP_ITC.1)

WLANAS10:FTP_ITC.1.1

The TSF shall be capable of using IEEE 802.1X, [***Internet Protocol Security (IPsec)***], and [***no other protocols***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: 802.1X authentication server, audit server, [***no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

WLANAS10:FTP_ITC.1.2

The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

WLANAS10:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**syslog-ipsec communications, radius-ipsec communications**].

5.1.8.3 Inter-TSF Trusted Channel (WLAN Client Communications) (WLANAS10:FTP_ITC.1/Client)

WLANAS10:FTP_ITC.1.1/Client

The TSF shall be capable of using WPA3-Enterprise, WPA2-Enterprise and [***WPA3-SAE-PK***] as defined by IEEE 802.11-2020 to provide a trusted communication channel between itself and

WLAN clients that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

WLANAS10:FTP_ITC.1.2/Client

The TSF shall permit the authorized IT entities to initiate communication via the trusted channel.

WLANAS10:FTP_ITC.1.3/Client

The TSF shall initiate communication via the trusted channel for no services.

5.1.8.4 Inter-TSF Trusted Channel (VPN Communications) (VPNGW12:FTP_ITC.1/VPN)

VPNGW12:FTP_ITC.1.1/VPN

The TSF shall be capable of using IPsec to provide a communication channel between itself and authorized IT entities supporting VPN communications that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

VPNGW12:FTP_ITC.1.2/VPN

The TSF shall permit the authorized IT entities to initiate communication via the trusted channel

VPNGW12:FTP_ITC.1.3/VPN

The TSF shall initiate communication via the trusted channel for [no functions].

5.1.8.5 Trusted Path - per TD0639 (NDcPP22e:FTP_TRP.1/Admin)

NDcPP22e:FTP_TRP.1.1/Admin

The TSF shall be capable of using [***SSH***] to provide a communication path between itself and authorized remote Administrators that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure and provides detection of modification of the channel data.

NDcPP22e:FTP_TRP.1.2/Admin

The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Admin

The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey
	AVA_VLA.1: Additional Flaw Hypotheses

Table 3 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d
The developer shall provide a functional specification.

ADV_FSP.1.2d
The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c
The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c
The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c
The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c
The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e
The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d
The developer shall provide operational user guidance.

AGD_OPE.1.1c
The operational user guidance shall describe, for each user role, the user accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2c
The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c
The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4c
The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c
The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c
The operational user guidance shall, for each user role, describe the security measures to be

followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1c

The TOE shall be labelled with its unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d
The developer shall provide the TOE for testing.

ATE_IND.1.1c
The TOE shall be suitable for testing.

ATE_IND.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e
The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d
The developer shall provide the TOE for testing.

AVA_VAN.1.1c
The TOE shall be suitable for testing.

AVA_VAN.1.1e
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e
The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e
The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Communication
- Cryptographic support
- Identification and authentication
- Security management
- Packet Filtering
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

NDcPP22e:FAU_GEN.1:

WLANAS10:FAU_GEN.1/WLAN:

NDcPP22e:FAU_GEN.2:
The vendor's Administrative Guidance enumerates the TOE's audit records (generated by the TOE, as the TOE has only a single component and is not a distributed TOE). The TOE identifies cryptographic keys in audit records (records related to the generation/import, changing, or deleting of keys) by their issuer and subject Distinguished Names.

VPNGW12:FAU_GEN.1/VPN:
The TOE's VPN gateway functionality uses the same underlying audit mechanism (rsyslog) to generate its audits, and thus the TOE transmits VPN audits the same way as it does base-NDcPP audits.

NDcPP22e:FAU_STG_EXT.1:
The TOE transmits audit data via syslog transmitted within an IPsec tunnel. The TOE has four gigabytes of internal storage for audit records and should the TOE exhaust this storage space, it overwrites the oldest previous audit records with the new audit records.

The TOE is a standalone TOE that stores audit data locally, and the TOE's logd will rotate logs and once out of space, delete the oldest logs in order to make room for newer logs.

The vendor has designed the TOE to accumulate audit logs while fielded and, upon detecting it has regained network connectivity (typically after returning from the field), to transmit its audit records to the administrator defined remote syslog server. If the TOE can establish an IPsec connection to the admin configured syslog server, it transmits audit records in real-time to the syslog server (while still storing the audit records locally).

6.2 Cryptographic support

NDcPP22e:FCS_CKM.1:

VPNGW12:FCS_CKM.1/IKE:
The TOE generates the asymmetric keys listed in the table below. The TOE generated ECDSA key pairs per FIPS 186-4 Appendix B.4.2 ("Testing Candidates") and does not introduces any TOE-specific extensions, processing or alternative implementations. However, the TOE does diverge from the sole "**should**" found in FIPS 186-4 section B.4.2 (within **Output:** step 2,). The TOE instead internally logs any error encountered during public/private key pair generation and does not output any *d* or *Q* values (in order to fail secure).

Purpose	SFR	Scheme	Size
IKE authentication	VPNGW12: FCS_IPSEC_EXT.1.13	ECDSA	P-384
IKE key exchange	VPNGW12: FCS_IPSEC_EXT.1.11	ECDSA	P-256, P-384
WPA3-SAE ECDHE	WLANAS10:FCS_CKM.1/WPA	ECDH	P-256, P-384
SSH authentication	NDcPP22e:FCS_SSHS_EXT.1.5	ECDSA	P-384

SSH key exchange	NDcPP22e:FCS_SSHS_EXT.1.7	ECDH	P-256, P-384

WLANAS10:FCS_CKM.1/WPA:
The TOE establishes the GTK and PTK in accordance with IEEE 802.11-2020 and IEEE 802.11ax-2021.

The TOE derives the PTK from the PMK, however, the details of the PMK differs based upon mode. When operating in WPA3-SAE mode, the TOE establishes the PMK from SAE's dragonfly key exchange.

When operating in WPA3/WPA2-Enterprise mode, the TOE receives the PMK from the Enterprise RADIUS server (the server establishes the PMK from the EAP-TLS exchange).

In both modes, the TOE derives the GTK from the GMK (which the TOE randomly generates) and nonces. The TOE distributes the GTK to wireless clients in an EAPOL-Key frame wrapped using AES Key Wrap in accordance with the IEEE standards.

Upon a successful 4-way handshake, the Authenticator will allow for WLAN data to pass through the system to the Controller in a tunnel architecture or to intended destination in distributed architecture.

The PTK (total 384 bits) is derived into three parts. The second part is KEK and used to encrypt GTK to be sent as 3rd message in WPA2 handshake. Third part is TK, which is actually used to encrypt/decrypt communication between both AP and Client.

The TOE incorporates the NXP (formerly Marvell) 88W8997 Wave 2 Wi-Fi System on Chip (SoC), which NXP subjected to Wi-Fi Alliance testing to demonstrate that the SoC (instantiated in a Test Bed Evaluation Kit) implements the IEEE 802.11-2012 standards correctly. Refer to the Wi-Fi Alliance certificates for compliance, https://www.wi-fi.org/certification.

Device	Wi-Fi Alliance Certificate
Datasoft RAP-117	WFA 72793

NDcPP22e:FCS_CKM.2:
Please see the table in NDcPP22e:FCS_CKM.1 above, which describes the asymmetric keys used for key establishment.

WLANAS10:FCS_CKM.2/GTK:
The TOE wraps the GTK with AES Key Wrap (in an EAPOL-Key frame) and will distribute the GTK after the 4-way handshake when a wireless client first connects as well as after any update to the GTK.

WLANAS10:FCS_CKM.2/PMK:
As described above, the TOE receives the PMK in the EAP MS-MPPE-Recv-Key and MS-MPPE-Send-Key RADIUS attributes contained within a RADIUS Access-Accept packet (ultimately transmitted by the Enterprise RADIUS server) within an IPsec protected channel.

NDcPP22e:FCS_CKM.4:
The TOE includes the following cryptographic keys

Key	Storage (RAM/Flash)	Encrypted/ Plaintext	Destruction and when
IKE auth keys	RAM	Plaintext	Cleared w/ zeros after use
IKE auth keys	Flash	Plaintext	Stored persistently in the TOE's data partition, and cleared w/ a four-pass overwrite (RNG and zeros) upon zeroization
IKE/ESP SA keys	RAM	Plaintext	Cleared w/ zeros after use
WPA3-SAE ECDH keys	RAM	Plaintext	Cleared w/ zeros after use
WPA2/3 keys	RAM	Plaintext	Cleared w/ zeros after use
SSH host key	RAM	Plaintext	Cleared w/ zeros after use
SSH host key	Flash	Plaintext	Stored persistently in the TOE's data partition, and cleared w/ a four-pass overwrite (RNG and zeros) upon zeroization
SSH session	RAM	Plaintext	Cleared w/ zeros after use

FCS_COP:

The TOE's OpenSSL (version 3.1.0 executing on the TOE's i.MX 6UltraLite MCIMX6G2 Processor) library possesses the following cryptographic algorithm certificates:

Requirements	Functions	CAVP Cert
	Cryptographic key generation	
NDcPP22e:FCS_CKM.1	ECC schemes using 'NIST curves' P-256, P-384	A3743
	IKE Peer Auth Cryptographic key generation	
VPNGW12:FCS_CKM.1/IKE	ECC schemes using 'NIST curves' P-384	A3743
	Cryptographic key establishment/distribution	
NDcPP22e:FCS_CKM.2	Elliptic curve-based key establishment schemes: P-256, P-384	A3743
WLANAS10:FCS_CKM.2.1/GTK	AES KW (128 and 256 bits)	A3743
	SSH Encryption/Decryption	
NDcPP22e:FCS_COP.1/DataEncryption	AES GCM (256 bits)	A3743
	IPsec/ESP Encryption/Decryption	
VPNGW12:FCS_COP.1/DataEncryption	AES CBC (256 bits)	A3743
	Cryptographic hashing	
NDcPP22e:FCS_COP.1/Hash	SHA-256/384/512 (digest sizes 256, 384 and 512 bits)	A3743
	Keyed-hash message authentication	
NDcPP22e:FCS_COP.1/KeyedHash	HMAC-SHA-384 (key and output MAC size 384)	A3743
	Cryptographic signature services	
NDcPP22e:FCS_COP.1/SigGen	Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical curve P-384	A3743
	Random bit generation	
FCS_RBG_EXT.1	CTR_DRBG (AES) with HW based noise sources (256 bits)	A3743

The TOE's Kernel Cryptography (version 5.4 executing on the TOE's i.MX 6UltraLite MCIMX6G2 Processor) library possesses the following cryptographic algorithm certificates:

Requirements	Functions	CAVP Cert
	Encryption/Decryption (802.11 Wi-Fi)	
WLANAS10:FCS_COP.1/DataEncryption	AES CCMP and GCMP (128 and 256 bits)	A3754
	IPsec/ESP Encryption/Decryption	
VPNGW12:FCS_COP.1/DataEncryption	AES GCM (256 bits)	A3754

NDcPP22e:FCS_COP.1/DataEncryption:

The TOE supports AES-256 in the GCM modes in SSH.

VPNGW12:FCS_COP.1/DataEncryption:
The TOE supports AES-256 CBC and GCM for all of its IPsec connections (with clients, remote syslog, and RADIUS server). The TOE performs IKE/IPsec AES-GCM using its Kernel Cryptography, while performs AES-CBC using its OpenSSL library.

WLANAS10:FCS_COP.1/DataEncryption:
The TOE supports AES-CBC in order to comply with FCS_IPSEC_EXT.1 requirement and also supports AES-128/256 CCMP and AES-256 GCMP modes of feedback for 802.11 wireless clients. The TOE encrypts and decrypts Wi-Fi frames using its RAP Kernel Cryptography AES implementation.

NDcPP22e:FCS_COP.1/Hash:
The TOE makes use of hashing within its SSH connections (for remote administration), for the integrity of IPsec/ESP traffic, as part of WPA2/3 PRF functionality, for signature generation and verification (both IKE peer authentication and trusted updates), and finally internally uses SHA-512 for hashing administrator passwords before storing them.

NDcPP22e:FCS_COP.1/KeyedHash:
The TOE uses HMAC keys sized 384 bits with hashes SHA-384 with block size 1024 bits and with output MAC length 384 respectively.

NDcPP22e:FCS_COP.1/SigGen:
The TOE generates ECDSA signatures (during IPsec/IKE peer authentication) using curves P-384. The TOE also verifies ECDSA signatures during IKE peer authentication and when verifying trusted updates.

NDcPP22e:FCS_IPSEC_EXT.1:

VPNGW12:FCS_IPSEC_EXT.1:
The following IPSEC TSS descriptions address the collective requirements of the base protection profile and those of the modules.

FCS_IPSEC_EXT.1.1:
The TOE implements the IPsec protocol as specified in RFC 4301, and the TOE matching incoming and outgoing traffic against packet filtering and SPD rules to determine whether traffic should bypass ESP encryption (BYPASS), have ESP encryption applied (PROTECT), or whether the traffic should be dropped (DISCARD). The administrator can configure these by specifying the syslog and radius server to which the TOE connects.

The TOE routes all packets through the kernel's IPsec interface (ipsec0) when any of its VPNs are active. The kernel compares packets routed through this interface to the SPDs configured for the VPN to determine whether to PROTECT, BYPASS, or DISCARD each packet. The vendor designed the TOE, to allow no manual SPD configuration beyond specifying the IP addresses of the syslog and RADIUS server. Consequently, the TOE protects all traffic between VPN clients and TOE traffic to the syslog and RADIUS servers.

FCS_IPSEC_EXT.1.3:
The TOE supports only tunnel mode.

FCS_IPSEC_EXT.1.4:
The TOE implements both the AES-CBC-256 and AES-GCM-256 ciphers and implements the truncated HMAC-SHA-384 (which is truncated to 192 bits) algorithm for ESP integrity (the TOE uses HMAC-SHA-384 only when paired with the AES-CBC 256 cipher). The TOE's OpenSSL library implements the AES-CBC and HMAC-SHA-384 algorithms, while the TOE's Kernel Cryptography implements the AES-GCM algorithm.

FCS_IPSEC_EXT.1.5:
The TOE implements only IKEv2.

FCS_IPSEC_EXT.1.6:
The TOE uses AES-CBC-256 or AES-GCM-256 to encrypt its IKEv2 SAs.

FCS_IPSEC_EXT.1.7:

The TOE allows an administrator to provision the TOEs IKEv2 SA lifetime to a value between 3 and 24 hours.

FCS_IPSEC_EXT.1.8:
The TOE allows an administrator to provision the TOEs ESP SA lifetime to a value between 1 and 8 hours.

FCS_IPSEC_EXT.1.9:
The TOE supports key exchange groups DH19 and DH20 and generates a secret "x" of size 256 or greater bits,.

FCS_IPSEC_EXT.1.10:
The TOE generates IKEv2 nonces using its DRBG, and for DH19 and DH20, the TOE generates a 256 bit and 384 bit long nonce, respectively. Those lengths represent double the security strength.

FCS_IPSEC_EXT.1.11:
By default, the TOE supports DH20 (ECP-384) but allows an administrator to provision the TOE to also support DH19 (ECP-256) as well.

FCS_IPSEC_EXT.1.12:
The TOE only allows SA cipher strengths of 256 bits, hence the TOE's design inherently prevents a situation in where the ESP SA cipher strength exceeds that of theIKEv2 SA.

FCS_IPSEC_EXT.1.13:
The TOE supports ECDSA certificates for IKE peer authentication.

FCS_IPSEC_EXT.1.14:
The TOE supports Distinguished Name checking of VPN client certificates and checking of SAN:IPv4 (IPv4 addresses in the Subject Alternative Name) for syslog and RADIUS peer certificates.

NDcPP22e:FCS_RBG_EXT.1:
The TOE seeds its AES-256 CTR_DRBG using a 384-bit seed from a hardware entropy source.

NDcPP22e:FCS_SSHS_EXT.1:

NDcPP22e:FCS_SSHS_EXT.1.2:
The TOE supports only ECDSA client certificates and matches an SSH client's presented public key with one within the TOE's authorized_keys file. The TOE also supports password-based authentication, and in the absence of a presented public key, the TOE prompts the client to supply a username and password.

NDcPP22e:FCS_SSHS_EXT.1.3:
The TOE inspects incoming SSH packets to check for those larger than 263,144 bytes in size and drops such packets.

NDcPP22e:FCS_SSHS_EXT.1.4:
The TOE supports the AES-256-GCM cipher mode.

NDcPP22e:FCS_SSHS_EXT.1.5:
The TOE's supports an ECDSA host key (size P-384) for when the TOE uses pubkey authentication to authenticate to connecting SSH clients.

NDcPP22e:FCS_SSHS_EXT.1.6:
The TOE supports the "implicit" mode of integrity associated with AES-GCM.

NDcPP22e:FCS_SSHS_EXT.1.7:
The TOE supports ecdh-sha2-nistp256 and ecdh-sha2-nistp384.

NDcPP22e:FCS_SSHS_EXT.1.8:
The TOE supports rekey limits of 1 hour and 0.5 Gigabyte and initiates a rekey when it encounters either threshold.

6.3 Identification and authentication

WLANAS10:FIA_8021X_EXT.1:
The TOE adheres to the 802.1X-2010 standard in supporting EAPOL for wireless authentication (IEEE 802.11) and does not support other 802.1X methods included in the standard (e.g., Token Ring, FDDI, MACsec, etc.). The vendor has performed research and testing during product development to ensure compatibility and interoperability.

NDcPP22e:FIA_AFL.1-Notes:
The TOE allows the administrator to configure an admin lock out time between 5 to 120 minutes. The TOE tracks failed password authentication attempts for each user and will lock out the user for the administrator configured time, or until another administrator unlocks the user.

The TOE ensures that while failed logins results in lockout of remote users (administrators), the TOE does not lock out local administrators (those accessing the TOE via its USB interface) after failed logins.

NDcPP22e:FIA_PMG_EXT.1:
The TOE supports passwords with a minimum and maximum length of between 6 and 16 characters consisting of the 95 ASCII printable characters (i.e., upper and lower case letters, numbers and the following special characters: [***'!', '@', '#', '$', '%', '^', '&', '*', '(', ')', /= + - _ ` ~ | / [{ } ~ ' ; : / ? . > , <***/] ;).

WLANAS10:FIA_UAU.6:
The TOE requires the administrator to provide their current password in addition to his or her new password as part of process for an administrator to change his or her password.

NDcPP22e:FIA_UAU.7:
The TOE obscures feedback to the local administrative user while authenticating.

NDcPP22e:FIA_UAU_EXT.2:

NDcPP22e:FIA_UIA_EXT.1:
The TOE provides both username/password as well as pubkey authentication for administrators (who connect via SSH). The TOE allows no actions prior to successful authentication (and successful authentication consists of either a valid pubkey authentication or a correct username/password combination). The TOE provides the same SSH authentication to local and remote administrators; however, access through the TOE's Ethernet port constitutes remote administration and access through the TOE's USB interface constitutes local administration.

NDcPP22e:FIA_X509_EXT.1/Rev:
The TOE checks the validity (expiration as well as checking for explicit curves) of X.509 certificates during loading and during IKE authentication. The TOE enforces no requirements on extendedKeyUsage fields of the peer's certificate. The TOE checks revocation by checking the Certificate Revocation List (CRL) of the issuing CA. The TOE attempts to check certificate revocation status via CRLs when performing IKE peer/client authentication. The TOE requires that the IKE peer/client always provide a full certificate chain.

NDcPP22e:FIA_X509_EXT.2:

VPNGW12:FIA_X509_EXT.2:
The administrator can configure the root CA used during IKE authentication. If the TOE cannot establish a connection with a revocation server to check the status of a certificate in question, the TOE will not accept the certificate (the TOE rejects the certificate as invalid).

NDcPP22e:FIA_X509_EXT.3:
The TOE includes a Common Name (CN) and SAN:IPv4 in its CSR.

6.4 Security management

NDcPP22e:FMT_MOF.1/Functions:
An administrator can configure the external syslog server.

NDcPP22e:FMT_MOF.1/ManualUpdate:
The TOE allows only administrators to initiate a manual update of the TOE's firmware.

NDcPP22e:FMT_MTD.1/CoreData:
The TOE provides no access to any services prior to login other than clearing keys (through a physical switch on the TOE's exterior). This prevents non-administrative users from accessing TOE services.

NDcPP22e:FMT_MTD.1/CryptoKeys:

VPNGW12:FMT_MTD.1/CryptoKeys:

The TOE allows only security administrators to manage (i.e., import or delete) root CAs (used during IKE certificate authentication) and the certificates the TOE uses to authenticate itself to IKE peers. This represents the TOE's trust store for X.509v3 certificates. The TOE restricts changes to its trust store to authenticated administrators, who can make changes using the Device Provisioning Application (DPA).

NDcPP22e:FMT_SMF.1:
The TOE makes its administrative account management services available through its local (USB) and remote (Ethernet) administrative interfaces. These services include creation, deletion, and unlocking of administrative accounts. The TOE also includes those administrative services listed in the SFR in section 5.1.4.6

WLANAS10:FMT_SMF.1/AccessSystem:
The TOE supports WPA2-Enterprise mode and support both WPA3-Enterprise and WPA-SAE modes in 2.4 and 5 GHz radio frequencies. The TOE rejects any connections from clients that do not offer a security type matching those the TOE provides. The TOE allows an administrator to use the Device Provisioning Application (DPA) to configure the Security type (WPA2 or WPA3), Authentication protocol (SAE or Enterprise), the SSID, the Transmit power level, and the client authentication credential (SAE passphrase).

VPNGW12:FMT_SMF.1/VPN:
The TOE provides all management functions listed in VPNGW12:FMT_SMF.1/VPN through both its local (USB) and remote (Ethernet) management interfaces. Those include definition of packet filtering rules, associate of those rules to network interfaces, and ordering of those rules by priority.

NDcPP22e:FMT_SMR.2:
The supports only local and remote administrator and places no restrictions on these roles other than exempting local administration from incorrect password lock out.

WLANAS10:FMT_SMR_EXT.1:
The TOE prohibits administration sessions from Wireless clients.

6.5 Packet Filtering

VPNGW12:FPF_RUL_EXT.1:

VPNGW12:FPF_RUL_EXT.1.1:
The TOE's boot process brings up firewall rules (netfilter) prior to bringing up networking interfaces, and as such cannot send unfiltered traffic. The TOE's netfilter kernel process bears responsibility for processing network packets and processes each packet against the netfilter rules governing each input and output chain. Should netfilter fail, because it executes within the kernel, its failure would trigger a kernel panic and result in the TOE restarting.

VPNGW12:FPF_RUL_EXT.1.2:

VPNGW12:FPF_RUL_EXT.1.3:

VPNGW12:FPF_RUL_EXT.1.4:
The TOE implements a packet filtering policy implementation that can use the following fields in these RFC protocols:

The TSF shall allow the definition of Packet Filtering rules (permit, discard, and log) using the following network protocols and protocol fields:

- IPv4 (RFC 791)
    - o source address
    - o destination address
    - o protocol
- IPv6 (RFC 2460)
    - o source address
    - o destination address
    - o next Header (protocol)
- TCP (RFC 793)
    - o source port

o destination port
- UDP (RFC 768)
o source port
o destination port.

The TOE only has a single Ethernet interface (beyond its wireless and USB interfaces). During development, the vendor determined compliance by examining the TOE's open source implementation to ensure compliance and by also performing limited independent testing to ensure that the implementation could correctly filter based upon the above protocols and protocol fields.

VPNGW12:FPF_RUL_EXT.1.5:
The TOE processes incoming packets in netfilter's chain applying the administrator defined rulesets in order. The TOE also includes a set of default rules, which restrict the TOE to the minimum necessary traffic needed for the WLAN (802.11 Wi-Fi) IPsec tunnel, SSH administration of the RAP, and the RAP's outgoing connections for syslog and RADIUS. The TOE also inspects packets to determine whether those packets are part of an established session, and if so, applies the administrator defined rulesets accordingly.

VPNGW12:FPF_RUL_EXT.1.6:
The TOE has a default discard rule which drops packets that match no existing or administrator defined rule, and the TOE's supports the full list of IPv4/IPv6 protocols and does not differ.

6.6 Protection of the TSF

NDcPP22e:FPT_APW_EXT.1:
The TOE stores administrative user SSH passwords hashed with SHA-256.

WLANAS10:FPT_FLS.1:

VPNGW12:FPT_FLS.1/SelfTest:
If the TOE fails a power-up self-test, fails noise source health tests during boot, or fails the image integrity check, the TOE will prevent further execution by halting its boot process, making key material inaccessible.

NDcPP22e:FPT_SKP_EXT.1:
The TOE stores IKE authentication certificates and SSH public/private keys and while the TOE provides administrative access to update or replace these keys, the TOE provides no method to view or output these values (even to authorized administrators). The TOE stores all keys in keys plaintext within the TOE's internal filesystem, to which administrators have no access.

NDcPP22e:FPT_STM_EXT.1:
The TOE makes use of time when generating audit records (which include a timestamp) and when performing IKE certificate validation (checking certificate validity), and the TOE contains a Real-Time Clock (RTC). After the administrator sets the TOE's clock during provisioning, the TOE can maintain accurate time using its internal RTC.

NDcPP22e:FPT_TST_EXT.1:

VPNGW12:FPT_TST_EXT.1:

WLANAS10:FPT_TST_EXT.1:

VPNGW12:FPT_TST_EXT.3:
The TOE runs a set of self-test for both its Kernel Cryptography and its OpenSSL library. The Kernel Cryptography self-tests cover AES and the OpenSSL library covers its AES, SHA hashing, HMAC, ECDSA, and DRBG algorithms. In each case, the self-test starts with known data (e.g., a known plaintext, key, and resulting ciphertext) and uses the data to ensure the algorithm works correctly. If any of these self-tests fail, the TOE flashes it LEDs and halts its boot. In addition to these tests, the TOE also ensures the integrity of its firmware image. The TOE's bootloader verifies the ECDSA signature on its firmware image before uncompressing and executing it. Finally, the TOE's noise source includes a health test to detect if the quality of the noise source degrades, and if so, halts outputting noise.

These tests together ensure that the TOE continues to operate correctly.

NDcPP22e:FPT_TUD_EXT.1:

VPNGW12:FPT_TUD_EXT.1:
The TOE provides an administrative command to check the installed firmware and further allows an administrator to updated the TOEs firmware by supplying a signed firmware update image. The TOE uses an existing, internal public key to verify the new image's signature (ensuring authenticity and integrity). The TOE does not support automatic checking of updates.

6.7 TOE access

NDcPP22e:FTA_SSL.3:
The TOE allows an administrator to configure a session inactivity time interval range of 3-30 minutes for inactive remote administrator sessions.

NDcPP22e:FTA_SSL.4:
The TOE allows administrators to terminate their remote or local sessions either through the exit command or by closing their SSH session.

NDcPP22e:FTA_SSL_EXT.1:
The TOE does not support local administrative session locking, but does support local administrative session termination (as described above).

NDcPP22e:FTA_TAB.1:
The TOE allows an administrator to set a banner that the TOE displays before each administrative session.

WLANAS10:FTA_TSE.1:
The TOE allows an administrator to configure the TOE to deny wireless client sessions based upon time and day (the TOE has only a single wireless interface, as opposed to WLAN systems with multiple wireless interfaces).

VPNGW12:FTA_VCM_EXT.1:
The TOE assigns private IP addresses to connected VPN clients.

6.8 Trusted path/channels

NDcPP22e:FTP_ITC.1/WLANAS10:FTP_ITC.1:
The TOE secures the connections to a remote syslog server and or to an 802.1X authentication server (RADIUS server) using IKEv2/IPsec. When establishing a connection with a RADIUS server, the TOE employs the 802.1X protocol within the IPsec tunnel.

WLANAS10:FTP_ITC.1/Client:
The TOE's typical deployment uses WPA3-SAE-PK, but the TOE also allows an administrator to configure use of WPA2 or WPA3 Enterprise. All three methods ensure a trusted channel between the TOE and its WLAN clients.

VPNGW12:FTP_ITC.1/VPN:
The TOE uses IPsec to protect its communications with VPN clients and with the two servers described above under NDcPP22e:FTP_ITC.1 (a syslog server and an enterprise RADIUS server). The TOE acts as an IKE/IPsec responder to VPN clients and an initiator when establishing a secure connection with a syslog or RADIUS server.

NDcPP22e:FTP_TRP.1/Admin:
The TOE supports remote administrators through interactive SSH sessions.