Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target

Version 0.6
09/18/2023

Prepared for:

CommScope Technologies LLC

130 Holger Way

San Jose, CA 95134

Prepared By:

Gossamer Laboratories

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 Ruckus SmartZone WLAN Controllers & Access Points with WIDS provided by CommScope Technologies LLC. The TOE is being evaluated as a wireless access system and wireless intrusion detection system.

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 – Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target

ST Version – Version 0.6

ST Date – 09/18/2023

1.2 TOE Reference

TOE Identification – Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3

Hardware versions:

- Wireless Controllers:

- Smart Zone 144
- Smart Zone 300 (SZ 300)
- Ruckus virtual SmartZone (includes vSZ) on VMware ESXi 7.0
- Ruckus virtual SmartZone – Data plane (vSZ-D) on VMware ESXi 7.0

- Access Points:
  - R650 (Including R650-WW)
  - R750 (including T750SE/T750 Omni and T750-WW)
  - R850

TOE Developer – CommScope Technologies LLC

Evaluation Sponsor – CommScope Technologies LLC

1.3 TOE Overview

The Target of Evaluation (TOE) is the Ruckus SmartZone WLAN Controllers & Access Points with WIDS , R5.2.1.3. The TOE is a distributed TOE. Ruckus Wireless Controller has been designed to eliminate the difficulties administrators experience with building and managing large-scale WLAN networks, to support several Wi-Fi access points and many concurrent Wi-Fi clients. Ruckus Wireless Controllers can support tens of thousands of Ruckus Smart Wi-Fi APs and hundreds of thousands of concurrent Wi-Fi subscribers. The Ruckus carrier-class management system provides feature-rich management of access points, such as RF management, load balancing, adaptive meshing and backhaul optimization and secure connectivity to all wireless clients.

1.4 TOE Description

Ruckus Wireless Controllers and Ruckus Smart Wi-Fi APs are deployed in a centralized deployment model. The NTP, Syslog, and Radius servers are part of the IT Environment in the following figures.

CENTRALIZED DEPLOYMENT MODEL

In a centralized deployment model client traffic always reaches the WLAN controller first via the AP before going to intended destination. See figure 1 and 2.

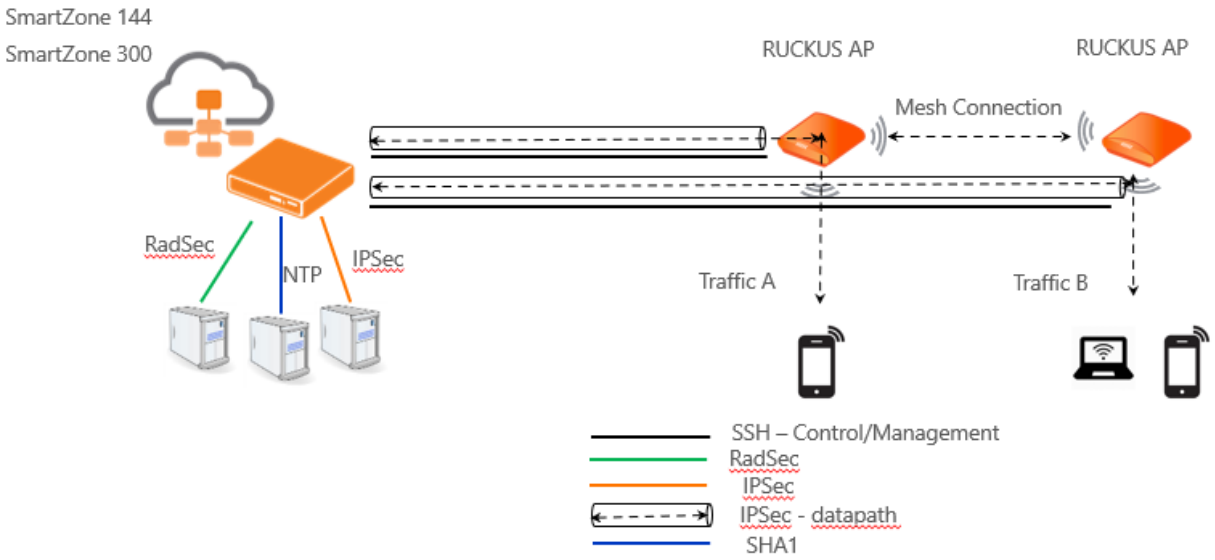

Figure 1 Centralized Deployment with Hardware

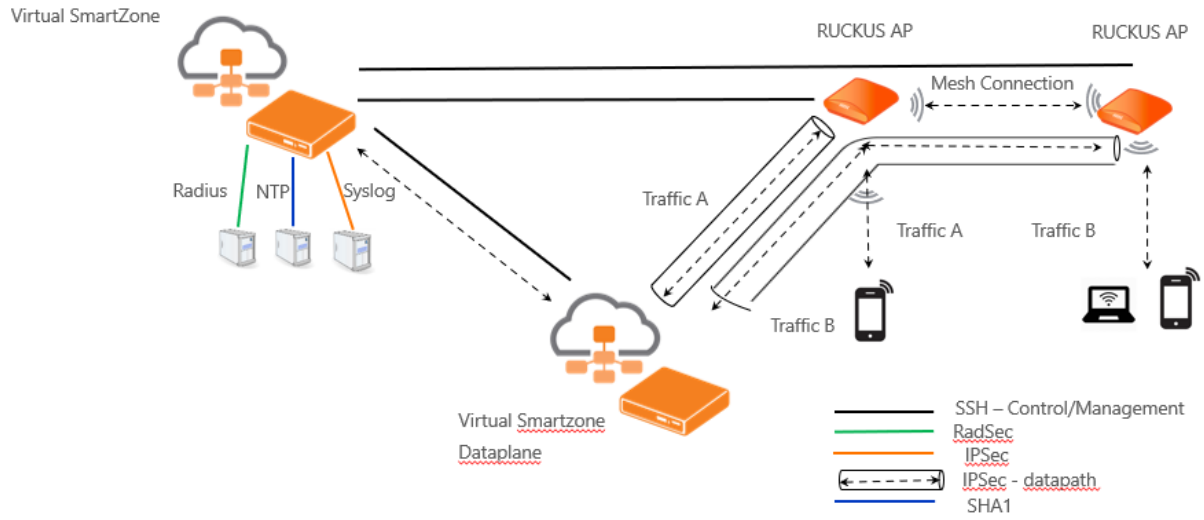

Figure 2 Centralized Deployment with Software

In Figure 1, the physical appliances consist of a Controller and an Access Point (AP) with the Dataplane (DP) built into the Controller. In Figure 2, the virtual deployment has a Controller, a separate DP and an AP.

Once authenticated as trusted nodes on the wired infrastructure, the access points provide the encryption service on the wireless network between themselves and the wireless client. The APs also communicate directly with the wireless controller for management purposes. The management traffic between Ruckus AP and Ruckus Wireless Controller is encrypted.

1.4.1 TOE Architecture

The Ruckus SmartZone controllers and Access points Solution (TOE) is a Wireless LAN access system (WLAN) and Wireless Intrusion Detection System (WIDS). The Wireless LAN access system and WIDS system defined in this ST is composed of multiple products operating together to provide secure wireless access to a wired and wireless network. The TOE provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement. The TOE has the following Access Point TOE components: R650, R750, and R850. The TOE also has the following Wireless Controllers: SmartZone 144, SmartZone 300 (SZ 300), virtual SmartZone (vSZ-E and vSZ-H hosted on a physical device), and virtual SmartZone – Data plane (vSZ-D hosted on a physical device). The TOE is a distributed TOE.

1.4.1.1 Physical Boundaries

The physical boundaries of the TOE consist of Wireless Controller and Access Points with WIDS running software version 5.2.1.3.

The specific hardware information is as follows:

Controller	CPU
Smart Zone 144 (SZ 144)	Intel(R) Xeon(R) CPU D-2143IT (Skylake)
Smart Zone 300 (SZ 300)	Intel(R) Xeon(R) CPU E5-2695 v3 (Haswell)
Ruckus virtual SmartZone (vSZ) on VMware ESXi 7.0	Intel(R) Xeon(R) Silver 4309Y CPU (Ice Lake)

Controller	CPU
Ruckus virtual SmartZone – Data plane (vSZ-D) on VMware ESXi 7.0	Intel(R) Xeon(R) Silver 4309Y CPU (Ice Lake)

Table 1 Controller CPU Identification

AP	CPU
R650 (Including R650-WW)	Qualcomm IPQ8071 (ARMv8)
R750 (Including T750SE/T750 Omni and T750-WW)	Qualcomm IPQ8076 (ARMv8)
R850	Qualcomm IPQ8078(ARMv8)

Table 2 AP CPU Identification

Non-TOE hardware/software required by the TOE for operation are the servers (RADIUS, Syslog, NTP, DHCP), wireless client, local and remote management computers.

The following configuration options are outside the evaluated configuration:

1) Internal captive portal
2) Soft-GRE to external gateway
3) FIPS/CC mode disabled
4) 802.11r
5) Clustering
6) Non-Proxy Authentication, Authorization & Accounting (AP directly talk to AAA)
7) GTP tunnel
8) SSH based AP administration (in the evaluated configuration, all administration is performed via the Controller)
9) Encrypted/Ruckus GRE

1.4.1.1.1 Wireless Controllers

The wireless controller serves client devices using secure authentication protocols, such as 802.1X/EAP. This is combined with policy-based data traffic steering which enterprises can optimize to forward all client traffic appropriately.

SZ 144
SmartZone™ 144 is a Scalable, Resilient, and High Performing Wireless LAN controller for Enterprises. It manages up to up to 2048 AP and 50,000 Clients per unit. SmartZoneOS' unique architecture enables SZ 144 to be deployed in multiple architectures like centralized and distributed traffic forwarding.

SZ 300
The SmartZone™ 300 (SZ 300) Flagship Large Scale WLAN Controller is designed for Service Provider and Large Enterprises, which prefer to use appliances. The SZ300 supports up to 10,000 AP and 100,000 Clients per unit.

vSZ
The Ruckus Virtual SmartZone™ (vSZ hosted on a physical device) is an NFV-based WLAN controller scale. The vSZ can be deployed in 2 modes, High Scale (vSZ-H) and Essentials (vSZ-E). High Scale supports up to 10,000 AP and 100,000 Clients per unit. Essentials supports up to 2048 AP and 50,000 Clients per unit.

vSZ-D
With the Virtual SmartZone Data Plane (vSZ-D hosted on a physical device), the Ruckus Virtual SmartZone platform launches data plane capabilities that enable tunneled WLAN architectures.

1.4.1.1.2 Access Points

The AP components can be centrally managed by the Ruckus Wireless Controller as part of a unified indoor/outdoor wireless LAN. Each AP supports a wide range of value-added applications.

Wireless communications between clients and APs is carried out using the IEEE 802.11 protocol standard. The 802.11 standard governs communication transmission for wireless devices. For this evaluation, the APs use a variation within 802.11a, 802.11ac, 802.11ax, 802.11b, 802.11g and 802.11n for wireless communication. The wireless security protocols that are to be used with the APs are 802.1X/802.1i.

The AP part of the TOE consists of the following component products:

AP	Location Type	Concurrent Users	User Data Rate
R650 (Including R650-WW)	Medium density	512	up to 2974 Mbps
R750 (Including T750SE/T750 Omni and R750-WW)	High density	1024	Up to 2400 Mbps
R850	High Density	1024	Up to 5984 Mbps

The T750SE is the 120 degree sector antenna variants of the R750 respectively and includes all of the same physical features.

The R650-WW and R750-WW are made up of the same hardware and software as the R650 and R750 respectively. The WW SKUs allow the user to choose the country code that determines the selection of radio channels for that country. The US SKUs are locked to radio channels allowed in the US.

The T750 Omni is the outdoor version of the R750

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- 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 configuration changes, administrative activities and other auditable events are audited both internally and 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. The TOE also provides a WIDS alerting capability. The WIDS alerts are generated based on signature based attacks and are related to APs and end user devices (EUDs). All WIDS alerts contain data to identify the malicious or rouge device.

1.4.1.2.2 Communication

The distributed TOE offers secure internal TSF communication via SSH and IPsec. Access Points and vSZ-Ds register to the WLAN controller over a dedicated channel and must be approved by the administrator to communicate with each other as parts of the distributed TOE.

1.4.1.2.3 Cryptographic support

The distributed TOE provides cryptographic functions for secure administration access via HTTPS and SSH; for communication between the distributed parts of the TOE via SSH and IPSec; for wireless communication via WPA3/WPA2 and for communication to external systems such as audit log servers via IPSec and RADIUS via TLS. Functions include Key generation, key establishment, key distribution, key destruction, cryptographic operations.

1.4.1.2.4 User data protection

The TOE provides a security policy to monitor authorized and unauthorized APs and EUDs.

1.4.1.2.5 Identification and authentication

The distributed TOE provides secure connectivity to the network for wireless clients via 802.1X authentication. Certificate based authentication is supported via external RADIUS server and password-based authentication is supported via the local authentication mechanism. The distributed TOE provides secure password-based authentication for remote administrators and X.509 certificate-based authentication for TOE components. The distributed TOE also provides strong password requirements that can be configured by the administrator 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.

1.4.1.2.6 Security management

TOE administrators manage the security functions of the TOE's distributed components from the SmartZone Controller, including software updates, via secure HTTPS connection over a web interface. Optionally SSH and the local console can also be used as a method to configure the system via the SmartZone controller. 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 access banner on the controller.

1.4.1.2.7 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 on self tests fail, a quarantine state is entered. All the components of the distributed TOE use X.509 certificates to authenticate and establish a secure connectivity amongst them. The TOE also allows configuration of timestamps via an NTP server. The TOE protects cryptographic keys and passwords from unauthorized access.

1.4.1.2.8 TOE access

A login banner is offered which provides the ability to have a custom warning/access policy message as per the organization needs. The TOE is capable of restricting wireless access based on TOE interface, 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.

1.4.1.2.9 Trusted path/channels

The TOE communicates to external components in a secure manner. The following secure channels are used to communicate externally – TLS for RADIUS, HTTPS for WebUI administration, SSH for CLI administration, IPsec for audit servers, and WPA3/WPA2 for wireless clients. The registration and joining of TOE components is performed over a dedicated channel. After registration, SSH is used for all management of the distributed TOE components (AP and vSZ-D) by the SmartZone Controller and IPSec is used for the data tunnel.

1.4.2 TOE Documentation

RUCKUS FIPS and Common Criteria Configuration Guide for SmartZone and APs, 5.2.1.3, Part Number: 800-72735-001 Rev D, October 2023.

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
- Package Claims:
    - PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) v1.0 (CFG_NDcPP-WIDS-WLANAS_V1.0)
        - Base-PP: collaborative Protection Profile for Network Devices', Version 2.2e, 23 March 2020 (NDcPP22e)
        - Module: PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 30 September 2020 (WIDS10)
        - Module: PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 19 April 2022 (WLANAS10)

Package	Technical Decision	Applied	Notes
CPP_ND_V2.2E	TD0738 - NIT Technical Decision for Link to Allowed-With List	Yes	
CPP_ND_V2.2E	TD0670 - NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	Yes	
CPP_ND_V2.2E	TD0639 - NIT Technical Decision for Clarification for NTP MAC Keys	Yes	
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	Yes	
CPP_ND_V2.2E	TD0634 - NIT Technical Decision for Clarification required for testing IPv6	Yes	
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	
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	Yes	
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	Yes	
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	Requirement not claimed
CPP_ND_V2.2E	TD0537 - NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	No	Requirement 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	Yes	
CPP_ND_V2.2E	TD0527 - Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	Yes	
MOD_WLAN_AS_v1.0	TD0680 - OS 4.2.1 Conformance Claims section updated to allow for MOD_WLAN_CLI_v1.0	No	OS PP not claimed
MOD_WLAN_AS_v1.0	TD0679 - Handling Standalone WLANAS TOEs with Single Interfaces	Yes	
MOD_WLAN_AS_v1.0	TD0651 - WLAN AS as Distributed and Non-distributed TOE	Yes	
MOD_WIDS_V1.0	TD0751 - Update to Wireless Threat Location Detection Scope	Yes	
MOD_WIDS_V1.0	TD0750 - Updates to FAU_SAA.1.2	Yes	
MOD_WIDS_V1.0	TD0613 - Update to Unauthorized Authentication Scheme	Yes	
MOD_WIDS_V1.0	TD0611 - Channels Outside Regulatory Domain	Yes	
MOD_WIDS_V1.0	TD0610 - Handling of non-allowlisted EUD	Yes	
MOD_WIDS_V1.0	TD0558 - Detection of excessive WPS negotiations	Yes	

2.1 Conformance Rationale

The ST conforms to the NDcPP22e/WIDS10/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/WIDS10/WLANAS10 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The NDcPP22e/WIDS10/WLANAS10 offers additional information about the identified security objectives, but that has not been reproduced here and the NDcPP22e/WIDS10/WLANAS10 should be consulted if there is interest in that material.

In general, the NDcPP22e/WIDS10/WLANAS10 has defined Security Objectives appropriate for wireless access and WIDS systems and as such are applicable to the Ruckus SmartZone WLAN Controllers & Access Points with WIDS 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.COMPONENTS_RUNNING (applies to distributed TOEs only)
For distributed TOEs, the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.

OE.CONNECTIONS TOE administrators will ensure that the TOE is installed in a manner that will allow the TOE to effectively enforce its policies on the network traffic of monitored 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.PROPER_ADMIN The administrator of the WIDS is not careless, willfully negligent or hostile, and administers the WIDS within compliance of the applied enterprise security policy.

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.

OE.VM_CONFIGURATION (applies to vNDs only)
For vNDs, the Security Administrator ensures that the VS and VMs are configured to
- reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and
- correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting).

The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration.
If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the NDcPP22e/WIDS10/WLANAS10. The NDcPP22e/WIDS10/WLANAS10 defines the following extended requirements and since they are not redefined in this ST the NDcPP22e/WIDS10/WLANAS10 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- WIDS10:FAU_ARP_EXT.1: Security Alarm Filtering
- NDcPP22e:FAU_GEN_EXT.1: Security Audit Generation
- WLANAS10:FAU_GEN_EXT.1: Security Audit Generation - per TD0651
- WIDS10:FAU_IDS_EXT.1: Intrusion Detection System - Intrusion Detection Methods
- WIDS10:FAU_INV_EXT.1: Environmental Inventory
- WIDS10:FAU_INV_EXT.2: Characteristics of Environmental Objects
- WIDS10:FAU_INV_EXT.3: Location of Environmental Objects
- WIDS10:FAU_RPT_EXT.1: Intrusion Detection System - Reporting Methods
- NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
- WIDS10:FAU_STG_EXT.1: Protected Audit Event Storage
- NDcPP22e:FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs
- NDcPP22e:FAU_STG_EXT.5: Protected Remote Audit Event Storage for Distributed TOEs
- WIDS10:FAU_WID_EXT.1: Wireless Intrusion Detection - Malicious Environmental Objects
- WIDS10:FAU_WID_EXT.2: Wireless Intrusion Detection - Passive Information Flow Monitoring
- NDcPP22e/WIDS10:FCO_CPC_EXT.1: Component Registration Channel Definition
- NDcPP22e:FCS_HTTPS_EXT.1: HTTPS Protocol
- NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0633
- NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
- WLANAS10:FCS_RADSEC_EXT.1: RadSec
- NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
- NDcPP22e:FCS_SSHC_EXT.1: SSH Client Protocol - per TD0636
- NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
- NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per TD0634 & TD0670
- NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication
- WLANAS10:FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication
- NDcPP22e:FIA_PMG_EXT.1: Password Management
- WLANAS10:FIA_PSK_EXT.1: Extended: Pre-Shared Key Composition
- NDcPP22e:FIA_UAU_EXT.2: Password-based Authentication Mechanism
- NDcPP22e:FIA_UIA_EXT.1: User Identification and Authentication
- NDcPP22e:FIA_X509_EXT.1/ITT: X.509 Certificate Validation
- NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation

- NDcPP22e: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
- 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
- WLANAS10:FPT_TST_EXT.1: TSF Testing
- NDcPP22e:FPT_TUD_EXT.1: Trusted update
- NDcPP22e:FTA_SSL_EXT.1: TSF-initiated Session Locking

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/WIDS10/WLANAS10. The refinements and operations already performed in the NDcPP22e/WIDS10/WLANAS10 are not identified (e.g., highlighted) here, rather the requirements have been copied from the NDcPP22e/WIDS10/WLANAS10 and any residual operations have been completed herein. Of particular note, the NDcPP22e/WIDS10/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/WIDS10/WLANAS10. The NDcPP22e/WIDS10/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 the Ruckus SmartZone WLAN Controllers & Access Points with WIDS TOE.

Requirement Class	Requirement Component
FAU: Security audit	WIDS10:FAU_ARP.1: Security Alarms
	WIDS10:FAU_ARP_EXT.1: Security Alarm Filtering
	NDcPP22e/WIDS10/WLANAS10:FAU_GEN.1: Audit Data Generation
	NDcPP22e:FAU_GEN.2: User identity association
	NDcPP22e:FAU_GEN_EXT.1: Security Audit Generation
	WLANAS10:FAU_GEN_EXT.1: Security Audit Generation - per TD0651
	WIDS10:FAU_IDS_EXT.1: Intrusion Detection System - Intrusion Detection Methods
	WIDS10:FAU_INV_EXT.1: Environmental Inventory
	WIDS10:FAU_INV_EXT.2: Characteristics of Environmental Objects
	WIDS10:FAU_INV_EXT.3: Location of Environmental Objects
	WIDS10:FAU_RPT_EXT.1: Intrusion Detection System - Reporting Methods
	WIDS10:FAU_SAA.1: Potential Violation Analysis
	NDcPP22e:FAU_STG_EXT.1: Protected Audit Event Storage
	WIDS10:FAU_STG_EXT.1: Protected Audit Event Storage
	WLANAS10:FAU_STG_EXT.1: Protected Audit Event Storage - per TD0651
	NDcPP22e:FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs
	NDcPP22e:FAU_STG_EXT.5: Protected Remote Audit Event Storage for Distributed TOEs
	WIDS10:FAU_WID_EXT.1: Wireless Intrusion Detection - Malicious Environmental Objects
	WIDS10:FAU_WID_EXT.2: Wireless Intrusion Detection - Passive Information Flow Monitoring
FCO: Communication	NDcPP22e/WIDS10:FCO_CPC_EXT.1: Component Registration Channel Definition
FCS: Cryptographic support	NDcPP22e:FCS_CKM.1: Cryptographic Key Generation

	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)
	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_HTTPS_EXT.1: HTTPS Protocol
	NDcPP22e:FCS_IPSEC_EXT.1: IPsec Protocol - per TD0633
	NDcPP22e:FCS_NTP_EXT.1: NTP Protocol
	WLANAS10:FCS_RADSEC_EXT.1: RadSec
	NDcPP22e:FCS_RBG_EXT.1: Random Bit Generation
	NDcPP22e:FCS_SSHC_EXT.1: SSH Client Protocol - per TD0636
	NDcPP22e:FCS_SSHS_EXT.1: SSH Server Protocol - per TD0631
	NDcPP22e:FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication - per TD0634 & TD0670
	NDcPP22e:FCS_TLSS_EXT.1: TLS Server Protocol
FDP: User data protection	WIDS10:FDP_IFC.1: Subset Information Flow Control
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_PSK_EXT.1: Extended: Pre-Shared Key Composition
	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/ITT: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.1/Rev: X.509 Certificate Validation
	NDcPP22e:FIA_X509_EXT.2: X.509 Certificate Authentication
	NDcPP22e:FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security management	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
	NDcPP22e:FMT_SMF.1: Specification of Management Functions - per TD0631
	WLANAS10:FMT_SMF.1/AccessSystem: Specification of Management Functions (WLAN Access Systems)

	WIDS10:FMT_SMF.1/WIDS: Specification of Management Functions (WIDS)
	NDcPP22e:FMT_SMR.2: Restrictions on Security Roles
	WLANAS10:FMT_SMR_EXT.1: No Administration from Client
FPT: Protection of the TSF	NDcPP22e:FPT_APW_EXT.1: Protection of Administrator Passwords
	WLANAS10:FPT_FLS.1: Failure with Preservation of Secure State
	NDcPP22e:FPT_ITT.1: Basic internal TSF data transfer protection - per TD0639
	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
	WLANAS10:FPT_TST_EXT.1: TSF Testing
	NDcPP22e: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
FTP: Trusted path/channels	NDcPP22e:FTP_ITC.1: Inter-TSF trusted channel - per TD0639
	WIDS10:FTP_ITC.1: Inter-TSF trusted channel
	WLANAS10:FTP_ITC.1: Inter-TSF Trusted Channel
	WLANAS10:FTP_ITC.1/Client: Inter-TSF Trusted Channel (WLAN Client Communications)
	NDcPP22e:FTP_TRP.1/Admin: Trusted Path - per TD0639
	NDcPP22e:FTP_TRP.1/Join: Trusted Path

Table 3 TOE Security Functional Components

5.1.1 Security audit (FAU)

5.1.1.1 Security Alarms (WIDS10:FAU_ARP.1)

WIDS10:FAU_ARP.1.1

The TSF shall display an alert to Authorized Administrator in sufficient detail to include identity of APs and EUDs involved, signal strength, accurate event timestamp, description of alert and severity level and [***no other actions***] upon detection of a potential security violation.

5.1.1.2 Security Alarm Filtering (WIDS10:FAU_ARP_EXT.1)

WIDS10:FAU_ARP_EXT.1.1

The TSF shall provide the ability to apply [**filter by classification**] to selectively exclude alerts from being generated.

5.1.1.3 Audit Data Generation (NDcPP22e/WLANAS10:FAU_GEN.1)

NDcPP22e/WLANAS10: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.

Requirement	Auditable Events	Additional Content
NDcPP22e/WLANAS10/:FAU_GEN.1	None	None
NDcPP22e:FAU_GEN.2	None	None
NDcPP22e:FAU_GEN_EXT.1	None	None
WLANAS10:FAU_GEN_EXT.1	None	None
NDcPP22e:FAU_STG_EXT.1	None	None
WLANAS10:FAU_STG_EXT.1	None	None
NDcPP22e:FAU_STG_EXT.4	None	None
WLANAS10:FAU_STG_EXT.4	None	None
NDcPP22e:FAU_STG_EXT.5	None	None
NDcPP22e:FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.
NDcPP22e:FCS_CKM.1	None	None
WLANAS10:FCS_CKM.1/WPA	None	None
NDcPP22e:FCS_CKM.2	None	None
WLANAS10:FCS_CKM.2/GTK	None	None
WLANAS10:FCS_CKM.2/PMK	None	None
NDcPP22e:FCS_CKM.4	None	None
NDcPP22e:FCS_COP.1/DataEncryption	None	None
WLANAS10:FCS_COP.1/DataEncryption	None	None
NDcPP22e:FCS_COP.1/Hash	None	None
NDcPP22e:FCS_COP.1/KeyedHash	None	None
NDcPP22e:FCS_COP.1/SigGen	None	None
NDcPP22e:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
NDcPP22e:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Protocol failures. Establishment or Termination of an IPsec SA.	Reason for failure. Reason for failure. Non-TOE endpoint of connection. Non-TOE endpoint of connection.
NDcPP22e:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server
WLANAS10:FCS_RADSEC_EXT.1	None	None
NDcPP22e:FCS_RBG_EXT.1	None	None
NDcPP22e:FCS_SSHC_EXT.1	Failure to establish an SSH session.	Reason for failure.
NDcPP22e:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.

NDcPP22e:FCS_TLSC_EXT.1	Failure to establish a TLS Session.	Reason for failure.
NDcPP22e:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
WLANAS10:FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange. Failed authentication attempt.	Provided client identity (e.g. Media Access Control [Media 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	None	None
WLANAS10:FIA_PSK_EXT.1	None	None
WLANAS10:FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
NDcPP22e:FIA_UAU.7	None	None
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/ITT	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.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	None	None
NDcPP22e:FIA_X509_EXT.3	None	None
NDcPP22e:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
NDcPP22e:FMT_MTD.1/CoreData	None	None
NDcPP22e:FMT_MTD.1/CryptoKeys	None	None
NDcPP22e:FMT_SMF.1	All management activities of TSF data.	None
WLANAS10:FMT_SMF.1/AccessSystem	None	None
NDcPP22e:FMT_SMR.2	None	None
WLANAS10:FMT_SMR_EXT.1	None	None
NDcPP22e:FPT_APW_EXT.1	None	None
WLANAS10:FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
NDcPP22e:FPT_ITT.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.
NDcPP22e:FPT_SKP_EXT.1	None	None

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	None	None
WLANAS10:FPT_TST_EXT.1	Execution of TSF self-test. Detected integrity violations.	None. The TSF code file that caused the integrity violation.
NDcPP22e:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None
NDcPP22e:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
NDcPP22e:FTA_SSL.4	The termination of an interactive session.	None
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.	None
NDcPP22e:FTA_TAB.1	None	None
WLANAS10:FTA_TSE.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.
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	None	None
NDcPP22e:FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None

Table 4 Audit events

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.

5.1.1.4 Audit Data Generation (WIDS) (WIDS10:FAU_GEN.1/WIDS)

WIDS10:FAU_GEN.1/WIDS.1

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;
c. [Auditable events listed in the Auditable Events table (Table 1);
d. Failure of wireless sensor communication].

Requirement	Auditable Events	Additional Content
WIDS10:FAU_ARP.1	Actions taken due to potential security violations	None
WIDS10:FAU_ARP_EXT.1	None	None
WIDS10:FAU_GEN.1/WIDS	None	None
WIDS10:FAU_IDS_EXT.1	None	None
WIDS10:FAU_INV_EXT.1	Presence of allowedlisted device	Type of device (AP or EUD), MAC Address
WIDS10:FAU_INV_EXT.2	None	None
WIDS10:FAU_INV_EXT.3	Location of AP or EUD	MAC Address, device type, classification of device, sensor(s) that detected device, signal strength as received by detecting sensor(s), proximity to detecting sensor(s)
WIDS10:FAU_RPT_EXT.1	None	None
WIDS10:FAU_SAA.1	None	None
WIDS10:FAU_STG_EXT.1	None	None
WIDS10:FAU_WID_EXT.1	Detection of rogue AP or EUD Detection of unauthorized SSID	None
WIDS10:FAU_WID_EXT.2	Sensor wireless transmission capabilities	Wireless transmission capabilities are turned on
WIDS10:FCO_CPC_EXT.1	None	None
WIDS10:FDP_IFC.1	None	None
WIDS10:FMT_SMF.1/WIDS	None	None

Table 5 Audit events

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.

5.1.1.5 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.

5.1.1.6 Security Audit Generation (NDcPP22e:FAU_GEN_EXT.1)

NDcPP22e:FAU_GEN_EXT.1.1

The TSF shall be able to generate audit records for each TOE component. The audit records generated by the TSF of each TOE component shall include the subset of security relevant audit events which can occur on the TOE component.

5.1.1.7 Intrusion Detection System - Intrusion Detection Methods (WIDS10:FAU_IDS_EXT.1)

WIDS10:FAU_IDS_EXT.1.1

The TSF shall provide the following methods of intrusion detection [***signature-based***].

5.1.1.8 Environmental Inventory (WIDS10:FAU_INV_EXT.1)

WIDS10:FAU_INV_EXT.1.1

The TSF shall determine if a given AP is authorized based on [***MAC addresses***]

WIDS10:FAU_INV_EXT.1.2

The TSF shall determine if a given EUD is authorized based on [***MAC addresses***]

WIDS10:FAU_INV_EXT.1.3

The TSF shall detect the presence of non-allow listed EUDs and APs in the Operational Environment.

5.1.1.9 Characteristics of Environmental Objects (WIDS10:FAU_INV_EXT.2)

WIDS10:FAU_INV_EXT.2.1

The TSF shall detect the

- Current RF band
- Current channel
- MAC Address
- Received signal strength
- Device detection timestamps
- Classification of APs and EUDs
- [***no other details***]

of all APs and EUDs within range of the TOE's wireless sensors.

WIDS10:FAU_INV_EXT.2.2

The TSF shall detect the following additional details for all APs within range of the TOE's wireless sensors:

- encryption
- number of connected EUDs
- Received frames/packets
- Beacon rate
- SSID of AP (if not hidden).

WIDS10:FAU_INV_EXT.2.3

The TSF shall detect the follow additional details for all EUDs within range of the TOE's wireless sensors:

- SSID and BSSID of AP it is connected to.
- DHCP configuration.

5.1.1.10 Location of Environmental Objects (WIDS10:FAU_INV_EXT.3)

WIDS10:FAU_INV_EXT.3.1

The TSF shall detect the physical location of APs and EUDs and [**allow-listed APs, allow-listed EUDS**] to within [**15**] feet of their actual location.

WIDS10:FAU_INV_EXT.3.2

The TSF shall detect received signal strength and [***no other characteristics***] of hardware operating within range of the TOE's wireless sensors.

5.1.1.11 Intrusion Detection System - Reporting Methods (WIDS10:FAU_RPT_EXT.1)

WIDS10:FAU_RPT_EXT.1.1

The TSF shall provide [***Syslog using [Syslog]***] for reporting of collected data.

WIDS10:FAU_RPT_EXT.1.2

The TSF shall provide the ability to import data, such as an allow list of APs and EUDs, and WIDS/WIPS configuration files from the system using [***custom API***].

5.1.1.12 Potential Violation Analysis (WIDS10:FAU_SAA.1)

WIDS10:FAU_SAA.1.1

The TSF shall be able to apply a set of rules for monitoring the wireless traffic and based upon these rules indicate a potential malicious action.

WIDS10:FAU_SAA.1.2

The TSF shall enforce the following rules for monitoring wireless traffic:

a. Accumulation or combination of [**no defined auditable events**] known to indicate a potential security violation,
b. Detection of non-allowlisted AP,
c. Detection of non-allowlisted EUD,
d. Detection of authorized EUD establishing peer-to-peer connection with any other EUD,
e. Detection of EUD bridging two network interfaces,
f. Detection of unauthorized point-to-point wireless bridges by allowlisted APs,
g. Alert generated by violation of user defined signature,
h. Detection of ICS connection,
~~i. Detection of traffic with excessive transmit power level,~~
j. Detection of MAC spoofing,
k. Detection of unauthorized AP broadcasting authorized SSIDs,
l. Detection of authorized AP broadcasting an unauthorized SSID,
m. Detection of allowlisted EUD connected to unauthorized SSID,
n. Detection of NULL SSID associations,
o. Detection of active probing,
p. Detection of packet flooding/DoS/DDoS,
q. Detection of RF-based denial of service,
r. Detection of deauthentication flooding,
s. Detection of disassociation flooding,
t. Detection of request-to-send/clear-to-send abuse,
u. Detection of unauthorized authentication scheme use,
v. Detection of unauthorized encryption scheme use,
w. Detection of unencrypted traffic,
x. Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations,
y. Detection of extremely high numbers of client devices using a particular allowlisted AP,
z. Detection of a high number of failed attempts to join the WLAN in a short period of time,
aa. Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic, such as Probes, Auths, and Assoc frames,
ab. Detection of the physical location of an identified WLAN threat by using triangulation,
ac. Detection of an SSID using weak/unsupported/disallowed encryption options,
ad. Detection of AP SSID larger than 32 bytes,
ae. [**no additional rules**].

(TD0558 & TD0750 applied)

5.1.1.13 Protected Audit Event Storage (NDcPP22e/WIDS10:FAU_STG_EXT.1)

NDcPP22e/WIDS10: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/WIDS10:FAU_STG_EXT.1.2

The TSF shall be able to store generated audit data on the TOE itself. In addition
[

- ***The TOE shall be a distributed TOE that stores audit data on the following TOE components: [Controllers],***
- ***The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [Controllers, Access Points (APs), vSZ-D].***]

NDcPP22e/WIDS10:FAU_STG_EXT.1.3

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

5.1.1.14 Protected Local Audit Event Storage for Distributed TOEs (NDcPP22e:FAU_STG_EXT.4)

NDcPP22e:FAU_STG_EXT.4.1

The TSF of each TOE component which stores security audit data locally shall perform the following actions when the local storage space for audit data is full: : [**The Controller shall *[overwrite previous audit records according to the following rule: [overwrite the oldest events first]***, [***no other action]]***].

5.1.1.15 Protected Remote Audit Event Storage for Distributed TOEs (NDcPP22e:FAU_STG_EXT.5)

NDcPP22e:FAU_STG_EXT.5.1

Each TOE component which does not store security audit data locally shall be able to buffer security audit data locally until it has been transferred to another TOE component that stores or forwards it. All transfer of audit records between TOE components shall use a protected channel according to [***FPT_ITT.1***]

5.1.1.16 Wireless Intrusion Detection - Malicious Environmental Objects (WIDS10:FAU_WID_EXT.1)

WIDS10:FAU_WID_EXT.1.1

The TSF shall distinguish between benign and malicious APs and EUDs based on if the APs and EUDs are authorized and [***no other method***].

WIDS10:FAU_WID_EXT.1.2

The TSF shall provide the ability to determine if a given SSID is authorized.

5.1.1.17 Wireless Intrusion Detection - Passive Information Flow Monitoring (WIDS10:FAU_WID_EXT.2)

WIDS10:FAU_WID_EXT.2.1

The TSF shall [***nonsimultaneously***] monitor and analyze network traffic matching the 802.11 monitoring SFP for all channels in the following RF frequencies:

- 2.4 GHz
- 5.0 GHz and
- [***no other domains***].

WIDS10:FAU_WID_EXT.2.2

The TSF shall provide wireless sensors to detect network traffic matching the802.11 monitoring SFP that [***can be configured to prevent transmission of data***].

WIDS10:FAU_WID_EXT.2.3

The TSF shall perform stateful frame inspection and log attacks spanning multiple frames.

5.1.2 Communication (FCO)

5.1.2.1 Component Registration Channel Definition (NDcPP22e/WIDS10:FCO_CPC_EXT.1)

NDcPP22e/WIDS10:FCO_CPC_EXT.1.1

The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

NDcPP22e/WIDS10:FCO_CPC_EXT.1.2

The TSF shall implement a registration process in which components establish and use a communications channel that uses [***A channel that meets the secure registration channel requirements in FTP_TRP.1/Join***] for at least TSF data.

NDcPP22e/WIDS10:FCO_CPC_EXT.1.3

The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.1.3 Cryptographic support (FCS)

5.1.3.1 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: [
- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.3,
- ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4,
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1,
- 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]].

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

WLANAS10:FCS_CKM.1/WPA.1

The TSF shall generate symmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm PRF-384 and [***no other algorithm***] 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 [***no other standards***].

5.1.3.3 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: [
- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, 'Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1',
- 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),
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, 'Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography',
- 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)].

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

WLANAS10:FCS_CKM.2/GTK.1

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.

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

WLANAS10:FCS_CKM.2/PMK.1

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.

5.1.3.1 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4) (v)SZ/vSZ-D

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 [single] overwrite consisting of [zeroes]***]

that meets the following: No Standard.

5.1.3.2 Cryptographic Key Destruction (NDcPP22e:FCS_CKM.4(1)) AP

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 [a pseudo-random pattern using the TSF's RBG]***];
- 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 [single] overwrite consisting of [a pseudo-random pattern using the TSF's RBG]***]

that meets the following: No Standard.

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

NDcPP22e:FCS_COP.1/DataEncryption.1

The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm AES used in [***CBC, CTR, GCM***] mode and cryptographic key sizes [***128 bits, 192 bits, 256 bits***] that meet the following: AES as specified in ISO 18033-3, [***CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772***].

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

WLANAS10:FCS_COP.1/DataEncryption.1

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 [***Galois-Counter Mode (GCM)***] modes and cryptographic key sizes 256 bits and [***128 bits, 192 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, [***GCM as specified in ISO 19772***].

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

NDcPP22e:FCS_COP.1/Hash.1

The TSF shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256, SHA-384, SHA-512***] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 10118-3:2004.

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

NDcPP22e:FCS_COP.1/KeyedHash.1

The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***] and cryptographic key sizes [**160, 256, 384, 512**] and message digest sizes [***160, 256, 384, 512***] bits that meet the following: ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.

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

NDcPP22e:FCS_COP.1/SigGen.1

The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [
- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits],
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits]]
that meet the following:
[***- For RSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,***
- For ECDSA schemes: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Section 6 and Appendix D, Implementing 'NIST curves' [P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4].

5.1.3.8 HTTPS Protocol (NDcPP22e:FCS_HTTPS_EXT.1)

NDcPP22e:FCS_HTTPS_EXT.1.1

The TSF shall implement the HTTPS protocol that complies with RFC 2818.

NDcPP22e:FCS_HTTPS_EXT.1.2

The TSF shall implement HTTPS using TLS.

NDcPP22e:FCS_HTTPS_EXT.1.3

If a peer certificate is presented, the TSF shall [***not require client authentication***] if the peer certificate is deemed invalid.

5.1.3.9 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 [***transport mode, 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-128 (RFC 3602), AES-CBC-192 (RFC 3602), AES-CBC-256 (RFC***

3602)] together with a Secure Hash Algorithm (SHA)-based HMAC [***HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512***].

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-128, AES-CBC-192, AES-CBC-256 (specified in RFC 3602)***].

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 [1-24] 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, 384**] bits.

NDcPP22e:FCS_IPSEC_EXT.1.10
The TSF shall generate nonces used in [***IKEv2***] exchanges of length [***at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash***].

NDcPP22e:FCS_IPSEC_EXT.1.11
The TSF shall ensure that IKE protocols implement DH Group(s) [***[14 (2048-bit MODP)], [20 (384-bit Random ECP)]***].

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 [***RSA, ECDSA***] that use X.509v3 certificates that conform to RFC 4945 and [***Pre-shared Keys***].

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: [***Distinguished Name (DN)***] and [***no other reference identifier type***].

5.1.3.10 NTP Protocol (NDcPP22e:FCS_NTP_EXT.1)

NDcPP22e:FCS_NTP_EXT.1.1
The TSF shall use only the following NTP version(s) [***NTP v4 (RFC 5905)***].

NDcPP22e:FCS_NTP_EXT.1.2
The TSF shall update its system time using [***Authentication using [SHA1] as the message digest algorithm(s);***].

NDcPP22e:FCS_NTP_EXT.1.3
The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

NDcPP22e:FCS_NTP_EXT.1.4
The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.1.3.11 RadSec (WLANAS10:FCS_RADSEC_EXT.1)

WLANAS10:FCS_RADSEC_EXT.1.1
The TSF shall implement RADIUS over TLS as specified in RFC 6614 to communicate securely with a RADIUS server.

WLANAS10:FCS_RADSEC_EXT.1.2
The TSF shall perform peer authentication using [***X.509v3 certificates***].

5.1.3.12 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 [***Hash_DRBG (any), 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 [***[1] software-based noise source, [2] 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.

5.1.3.13 SSH Client Protocol - per TD0636 (NDcPP22e:FCS_SSHC_EXT.1)

NDcPP22e:FCS_SSHC_EXT.1.1
The TSF shall implement the SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, [***5647, 5656, 6668***].

NDcPP22e:FCS_SSHC_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, [***no other method***].

NDcPP22e:FCS_SSHC_EXT.1.3
The TSF shall ensure that, as described in RFC 4253, packets greater than [**262144**] bytes in an SSH transport connection are dropped.

NDcPP22e:FCS_SSHC_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [***aes128-ctr, aes256-ctr, aes256-gcm@openssh.com***].

NDcPP22e:FCS_SSHC_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa***] as its public key algorithm(s) and rejects all other public key algorithms.

NDcPP22e:FCS_SSHC_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [***hmac-sha1, hmac-sha2-256, hmac-sha2-512, implicit***] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHC_EXT.1.7
The TSF shall ensure that [***diffie-hellman-group14-sha1, ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384, ecdh-sha2-nistp521***] are the only allowed key exchange methods used for the SSH protocol.

NDcPP22e:FCS_SSHC_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.

NDcPP22e:FCS_SSHC_EXT.1.9
The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [***no other methods***] as described in RFC 4251 section 4.1.

5.1.3.14 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, [***5647, 5656, 6668***].

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 [**262144**] 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: [***aes128-ctr, aes256-ctr, aes256-gcm@openssh.com***].

NDcPP22e:FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH public-key based authentication implementation uses [***ssh-rsa, rsa-sha2-256, rsa-sha2-512, 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 [***hmac-sha1, hmac-sha2-256, hmac-sha2-512, implicit***] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

NDcPP22e:FCS_SSHS_EXT.1.7
The TSF shall ensure that [***diffie-hellman-group14-sha1, ecdh-sha2-nistp256***] and [***ecdh-sha2-nistp384, ecdh-sha2-nistp521***] 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.

5.1.3.15 TLS Client Protocol Without Mutual Authentication - per TD0634 & TD0670 (NDcPP22e:FCS_TLSC_EXT.1)

NDcPP22e:FCS_TLSC_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,***
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]
and no other ciphersuites.

NDcPP22e:FCS_TLSC_EXT.1.2
The TSF shall verify that the presented identifier matches [***the reference identifier per RFC 6125 section 6***].

NDcPP22e:FCS_TLSC_EXT.1.3
When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [***Not implement any administrator override mechanism***].

NDcPP22e:FCS_TLSC_EXT.1.4
The TSF shall [***present the Supported Elliptic Curves/Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups***] in the Client Hello.

5.1.3.16 TLS Server Protocol Without Mutual Authentication (NDcPP22e:FCS_TLSS_EXT.1)

NDcPP22e:FCS_TLSS_EXT.1.1
The TSF shall implement [***TLS 1.2 (RFC 5246)***] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[***TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246,***
TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289]
and no other ciphersuites.

NDcPP22e:FCS_TLSS_EXT.1.2
The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [***TLS 1.1,***].

NDcPP22e:FCS_TLSS_EXT.1.3
The TSF shall perform key establishment for TLS using **[Diffie-Hellman parameters with size [3072 bits], ECDHE curves [secp384r1] and no other curves]].**

NDcPP22e:FCS_TLSS_EXT.1.4
The TSF shall support [***no session resumption or session tickets***].

5.1.4 User data protection (FDP)

5.1.4.1 Subset Information Flow Control (WIDS10:FDP_IFC.1)

WIDS10:FDP_IFC.1.1
The TSF shall enforce the 802.11 monitoring SFP on all IEEE802.11 a, b, g, n, ac frame types and subtypes between:

- authorized APs and authorized EUDs
- authorized APs and unauthorized EUDs
- unauthorized APs and authorized EUDs

5.1.5 Identification and authentication (FIA)

5.1.5.1 802.1X 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.

5.1.5.2 Authentication Failure Management (NDcPP22e:FIA_AFL.1)

NDcPP22e:FIA_AFL.1.1
The TSF shall detect when an Administrator configurable positive integer within [**1-100**] 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 Administrator defined time period has elapsed].

5.1.5.3 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 [**8**] and [**64**] characters.

5.1.5.4 Extended: Pre-Shared Key Composition (WLANAS10:FIA_PSK_EXT.1)

WLANAS10:FIA_PSK_EXT.1.1

The TSF shall be able to use pre-shared keys for [***IPSEC***, ***WPA3-SAE, IEEE 802.11 WPA2-PSK***].

WLANAS10:FIA_PSK_EXT.1.2

The TSF shall be able to accept text-based pre-shared keys that:

- are 22 characters and [***[up to 64 characters]***];
- are composed of any combination of upper and lower case letters, numbers, and special characters (that include: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')').

WLANAS10:FIA_PSK_EXT.1.3

The TSF shall be able to [a***ccept***] bit-based pre-shared keys.

5.1.5.5 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***]].

5.1.5.6 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.

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

NDcPP22e:FIA_UAU_EXT.2.1

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

5.1.5.8 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.

5.1.5.9 X.509 Certificate Validation (NDcPP22e:FIA_X509_EXT.1/ITT)

NDcPP22e:FIA_X509_EXT.1/ITT.1

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 two 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 [***no revocation method***].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - 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/ITT.2

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.

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

NDcPP22e:FIA_X509_EXT.1/Rev.1

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 [***the Online Certificate Status Protocol (OCSP) as specified in RFC 6960***]
- 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/Rev.2

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.

5.1.5.11 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 [***[RADSEC (RADIUS over TLS)]***].

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***].

5.1.5.12 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 [***Common Name, Country***].

NDcPP22e:FIA_X509_EXT.3.2
The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.1.6 Security management (FMT)

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

NDcPP22e:FMT_MOF.1/ManualUpdate.1
The TSF shall restrict the ability to enable the functions to perform manual updates to Security Administrators.

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

NDcPP22e:FMT_MTD.1/CoreData.1
The TSF shall restrict the ability to manage the TSF data to Security Administrators.

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

NDcPP22e:FMT_MTD.1/CryptoKeys.1
The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.1.6.4 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 manage the cryptographic keys,***
- Ability to configure the cryptographic functionality,
- Ability to configure the lifetime for IPsec SAs,
- Ability to configure the interaction between TOE components,
- Ability to set the time which is used for time-stamps,
- Ability to configure NTP,
- 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].

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

WLANAS10:FMT_SMF.1/AccessSystem.1
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

5.1.6.6 Specification of Management Functions (WIDS) (WIDS10:FMT_SMF.1/WIDS)

WIDS10:FMT_SMF.1/WIDS.1

The TSF shall be capable of performing the following management functions for WIDS functionality:

- Define an inventory of authorized APs based on [***MAC addresses***]
- Define an inventory of authorized EUDs based on MAC addresses
- Define rules for monitoring and alerting on the wireless traffic
- Define authorized SSID(s)
- Define authorized WLAN authentication schemes
- Define authorized WLAN encryption schemes
- [***[disable] transmission of data by wireless sensor,***
- ***Define attack signatures,***
- ***Define rules for overwriting previous packet captures,***
- ***Define the amount of time sensor monitors a specific [channel]***]

5.1.6.7 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.

5.1.6.8 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.

5.1.7 Protection of the TSF (FPT)

5.1.7.1 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.

5.1.7.2 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.

5.1.7.3 Basic internal TSF data transfer protection - per TD0639 (NDcPP22e:FPT_ITT.1)

NDcPP22e:FPT_ITT.1.1

The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE through the use of [***IPsec, SSH***].

5.1.7.4 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.

5.1.7.5 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 [***synchronize time with an NTP server***].

5.1.7.6 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: [**FIPS 140-2 power-up self-tests and integrity test for software and firmware**].

5.1.7.7 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, [***no other selftests***].

5.1.7.8 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 [***the most recently installed version of the TOE firmware/software***].

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.

5.1.8 TOE access (FTA)

5.1.8.1 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.

5.1.8.2 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.

5.1.8.3 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.

5.1.8.4 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.

5.1.8.5 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***].

5.1.9 Trusted path/channels (FTP)

5.1.9.1 Inter-TSF trusted channel - per TD0639 (NDcPP22e/WIDS10:FTP_ITC.1)

NDcPP22e/WIDS10: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, [***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.

NDcPP22e/WIDS10:FTP_ITC.1.2

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

NDcPP22e/WIDS10:FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [**audit server**].

5.1.9.2 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), Remote Authentication Dial In User Service (RADIUS) over Transport Layer Security (TLS)***], 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 [**802.1X authentication server, audit server**].

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

WLANAS10:FTP_ITC.1/Client.1
The TSF shall be capable of using WPA3-Enterprise, WPA2-Enterprise and [***WPA3-SAE, WPA2-PSK***] 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/Client.2
The TSF shall permit the authorized IT entities to initiate communication via the trusted channel.

WLANAS10:FTP_ITC.1/Client.3
The TSF shall initiate communication via the trusted channel for no services.

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

NDcPP22e:FTP_TRP.1/Admin.1
The TSF shall be capable of using [***SSH, HTTPS***] 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/Admin.2
The TSF shall permit remote Administrators to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1/Admin.3
The TSF shall require the use of the trusted path for initial Administrator authentication and all remote administration actions.

5.1.9.5 Trusted Path (NDcPP22e:FTP_TRP.1/Join)

NDcPP22e:FTP_TRP.1.1/Join
The TSF shall provide a communication path between itself and a joining component that is logically distinct from other communication paths and provides assured identification of [***both joining component and TSF endpoint***] and protection of the communicated data from modification **[*none*]**.

NDcPP22e:FTP_TRP.1.2/Join
The TSF shall permit [***the TSF***] to initiate communication via the trusted path.

NDcPP22e:FTP_TRP.1.3/Join
The TSF shall require the use of the trusted path for joining components to the TSF under environmental constraints identified in [**Admin Guide, Section "Joining vSZ-D to the vSZ Controller" and Section "AP Models that Support FIPS Mode"**].

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 6 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
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels

6.1 Security audit

The TOE generates audit records for start-up and shutdown of the TOE, all administrator actions, and for all the events identified in Table 4 and Table 5 Auditable Events. Audit records include date and time of the event, type of event, user identity that caused the event to be generated, the outcome of the event, as well as the additional content listed in column 3 of **Table 4** and **Table 5**. Any event that needs to be audited due to a user action is recorded with the identity of the user along with timestamps.

In the distributed TOE, the AP and vSZ-D components authenticate to the SZ/vSZ (Controller). Once an administrator allows the Controller to communicate to the AP and vSZ-D they form a distributed TOE. The AP and vSZ-D buffer their audit data locally and automatically forward it to the Controller via SSH in real time without any additional configuration needed. This buffer occurs in RAM. In the event that the buffer becomes full all new audits will be discarded although there is an age out mechanism to prevent this from happening. Any audits in the buffer that are not able to be sent to the controller within 30 minutes are deleted from the buffer. All audit messages are propagated via the Controller to an external audit server securely via IPSec in real-time, alternatively, the audit messages can be stored in the Controller itself. When stored locally, and local storage is full, the oldest audit records are overwritten. The Controller can store 14 archives of application logs with each log size of up to 100 MB. Only authorized administrators have access to the audit records.

In addition to audit records, the TOE also collects wireless intrusion detection system (WIDS) alerts. Each wireless sensor (AP) monitors wireless traffic, and forwards all data including alerts to the Controller in real time. The administrator is able to configure/enable these signature based WIDS alerts from the Controller and can filter the events collected by classification. The administrator can select WIDS alerts based on the following:

- Accumulation or combination of rules known to indicate a potential security violation (signature-based attacks),
- Detection of non-allowlisted AP,
- Detection of non-allowlisted EUD,
- Detection of authorized EUD establishing peer-to-peer connection with any other EUD,
- Detection of EUD bridging two network interfaces,
- Detection of unauthorized point-to-point wireless bridges by allowlisted APs,
- Alert generated by violation of user defined signature,
- Detection of ICS connection,
- Detection of traffic with excessive transmit power level,
- Detection of MAC spoofing,
- Detection of unauthorized AP broadcasting authorized SSIDs,
- Detection of authorized AP broadcasting an unauthorized SSID,
- Detection of allowlisted EUD connected to unauthorized SSID,

- Detection of NULL SSID associations,
- Detection of active probing,
- Detection of packet flooding/DoS/DDoS,
- Detection of RF-based denial of service,
- Detection of deauthentication flooding,
- Detection of disassociation flooding,
- Detection of request-to-send/clear-to-send abuse,
- Detection of unauthorized authentication scheme use,
- Detection of unauthorized encryption scheme use,
- Detection of unencrypted traffic,
- Detection of allowlisted EUD or AP that is using weak/outdated WLAN protocols and protocol implementations,
- Detection of extremely high numbers of client devices using a particular allowlisted AP,
- Detection of a high number of failed attempts to join the WLAN in a short period of time,
- Detection of the use of active WLAN scanners (e.g. wardriving tools) to generate WLAN traffic, such as Probes, Auths, and Assoc frames,
- Detection of the physical location of an identified WLAN threat by using triangulation,
- Detection of an SSID using weak/unsupported/disallowed encryption options,
- Detection of AP SSID larger than 32 bytes

The TOE synchronizes with an NTP server that is used to provide reliable time information for the audit records it generates.

The Security audit function satisfies the following security functional requirements:

- WIDS10:FAU_ARP.1: The TOE displays WIDS alerts to the administrator on the Controller and includes the identity of APs and EUDs involved, signal strength, accurate event timestamp, description of alert and severity level. A table of all the APs and clients detected by the monitoring APs by can be viewed under Report > Rogue Devices. This table also specifies if the rogue devices hit a configured WIDS event. The formal audits for the detection of these WIDS alerts can be viewed under Access Points > Monitoring APs > specific monitoring AP > Events.
- WIDS10:FAU_ARP_EXT.1: The TOE can filter WIDS alerts based on classification.
- NDcPP22e /WLANAS10:FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in Table 4. For cryptographic keys, the act of importing and deleting a key is audited with the key ID and the associated administrator account that performed the action is recorded.
- WIDS10:FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in Table 5.
- NDcPP22e:FAU_GEN.2: Any event that needs to be audited due to a user action is recorded with the identity of the user along with timestamps.
- NDcPP22e:FAU_GEN_EXT.1: All distributed TOE components generate audit records for security relevant actions performed on the component.
- WIDS10:FAU_IDS_EXT.1: The TOE performs signature based intrusion detection.
- WIDS10:FAU_INV_EXT.1: The TOE determines if a given AP or EUD is allowed based on its MAC address. It can detect allowed and non-allowed APs and EUDs. A table of all the APs and clients detected by the monitoring APs by can be viewed under Report > Rogue Devices which includes whether the device is allowlisted or not.
- WIDS10:FAU_INV_EXT.2: The TOE can detect all of the required characteristics of the APs and EUDs in its operating environment. This includes the current RF band, current channel, MAC Address, received signal strength, device detection timestamps, classification of APs and EUDs for all APs and EUDs within range of the TOE's wireless sensors. In addition for APs the details of encryption, number of connected EUDs,

received frames/packets, beacon rate, SSID of AP (if not hidden) are detected. In addition for EUDs the details of SSID and BSSID of AP it is connected to and DHCP configuration are detected..

- WIDS10:FAU_INV_EXT.3: The TOE can detect the physical location of APs and EUDs within 15 feet of their actual location as well as the signal strength of hardware operating within range of the TOE's wireless sensors. To ensure the physical location of APs and EUDs can be detected, the controller requires the use of 2 managed sensor in order to perform triangulation.
- WIDS10:FAU_RPT_EXT.1: The TOE uses syslog to report its WIDS alerts.
- WIDS10:FAU_SAA.1: The TOE provides a set of rules for WIDS monitoring. The rules are enumerated above. A WIDS rule for unauthorized SSIDs can be configured to detect a specific unauthorized SSID matching that set is by the administrator. A separate WIDS rule for any unauthorized SSIDs can be configured. In this case the authorized SSIDs are the ones explicitly configured for the WLANs managed by the TOE.
- NDcPP22e:FAU_STG_EXT.1: The APs and vSZ-D devices send their audits to the Controller in real-time. The Controller then interfaces with an audit server for transmission. This communication is protected with the use of IPsec.
- NDcPP22e:FAU_STG_EXT.4: The TOE can be configured to export audit records to an external syslog server. The communication must be protected with IPsec. When the local storage space for audit data is full, the TOE will overwrite the oldest records first.
- NDcPP22e:FAU_STG_EXT.5: The AP and vSZ-D buffer their security audit data locally and then send their audits to the Controller. All transfer of audit records between TOE components is protected using SSH.
- WIDS10:FAU_WID_EXT.1: The TOE can distinguish between benign and malicious APs and EUDs based on whether they have been allow-listed based on their MAC address. A WIDS rule for unauthorized SSIDs can be configured to detect an unauthorized SSID matching that set by the administrator. A separate WIDS rule for any unauthorized SSIDs can be configured. In this case the authorized SSIDs are the ones explicitly configured for the WLANs managed by the TOE.
- WIDS10:FAU_WID_EXT.2: The TOE monitor channels on the 2.4GHz and 5.0GHz network bands. The senor scans nonsimultaneoulsy, cycling through the channels based on the configured scan rate. The administrator can prevent transmissions by the sensor by placing the AP in a monitoring only mode.

6.2 Communication

The TOE requires the use of a dedicated channel for the AP and vSZ-D to register with a Controller. When an AP and vSZ-D discover a Controller via manual configuration or optionally via DHCP options, they will attempt to connect. Upon successful connection to the Controller, no data transfer is allowed between the Controller and AP/vSZD. An administrator must manually approve the AP/vSZ-D which enables data transfer between the Controller and AP/vSZ-D. An administrator also has the ability to manually revoke the connection between the Controller and AP/vSZ-D. After registering multiple APs to the same controller, the administrator has the option to enable a mesh configuration. In this configuration, any distributed TOE traffic is routed wirelessly from a mesh AP to a root AP wired directly to the Controller.

The Communication function satisfies the following security functional requirements:

- NDcPP22e/WIDS10:FCO_CPC_EXT.1: The connection between distributed parts of the TOE is made according to FTP_TRP.1/Join using a dedicated channel. In all cases, the administrator must approve or revoke the connection.

6.3 Cryptographic support

The TOE has several cryptographic libraries in each distributed component. The Controllers have version 5.2.1.3 of Ruckus Smartzone SSL Crypto Library and version 5.2.1.3 of Ruckus Smartzone Kernel Crypto Library. The associated CAVP certificates are:

Ruckus Smartzone SSL Crypto Library version 5.2.1.3:

Requirements	Functions	SZ Cert	vSZ Cert	vSZ-D Cert
	Cryptographic key generation			
FCS_CKM.1	**RSA schemes using cryptographic key sizes of 2048-bits, 3072-bits**	**C2082**	**A2457**	**A2458**
FCS_CKM.1	**ECC schemes using 'NIST curves'** **P-256, P-384, P-521**	**C2082**	**A2457**	**A2458**
FCS_CKM.1	**FFC schemes using cryptographic key sizes of 2048-bits, 3072-bits**	**C2082**	**A2457**	**A2458**
	Cryptographic key establishment/distribution			
FCS_CKM.2	**RSA-based key establishment schemes**	**Vendor Affirmed**	**Vendor Affirmed**	
FCS_CKM.2	**Elliptic curve-based key establishment schemes**	**A2456**	**A2457**	**A2458**
FCS_CKM.2	**Finite field-based key establishment schemes**	**A2456**	**A2457**	**A2458**
	Encryption/Decryption			
FCS_COP.1/ DataEncryption	**AES CBC and GCM (128, 192 and 256 bits)**	**C2082**	**A2457**	**A2458**
FCS_COP.1/ DataEncryption	**AES CTR (128 and 256 bits)**	**C2082**	**A2457**	**A2458**
	Cryptographic hashing			
FCS_COP.1/Hash	**SHA-1/256/384/512 (digest sizes 160, 256, 384 and 512 bits)**	**C2082**	**A2457**	**A2458**
	Keyed-hash message authentication			
FCS_COP.1/ KeyedHash	**HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (key and output MAC sizes 160, 256, 384 and 512 respectively)**	**C2082**	**A2457**	**A2458**

Requirements	Functions	SZ Cert	vSZ Cert	vSZ-D Cert
	Cryptographic signature services			
FCS_COP.1/SigGen	**RSA Digital Signature Algorithm (rDSA) (modulus 2048)**	**C2082**	**A2457**	**A2458**
FCS_COP.1/SigGen	**Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical curve size of 256, 384, or 521 bits**	**C2082**	**A2457**	**A2458**
	Random bit generation			
FCS_RBG_EXT.1	**CTR_DRBG (AES) and Hash_DRBG with HW based noise sources (256 bits)**	**C2082**	**A2457**	**A2458**

Ruckus Smartzone Kernel Crypto Library version 5.2.1.3

Requirements	Functions	SZ Cert	SZv Cert	
	Encryption/Decryption			
FCS_COP.1/ DataEncryption	**AES CBC (128 and 256 bits)**	**C2077**	**A3731**	**A3732**
	Cryptographic hashing			
FCS_COP.1/Hash	**SHA-1/256/384/512 (digest sizes 160, 256, 384 and 512 bits)**	**C2077**	**A3731**	**A3732**
	Keyed-hash message authentication			
FCS_COP.1/ KeyedHash	**HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (key and output MAC sizes 160, 256, 384 and 512 respectively)**	**C2077**	**A3731**	**A3732**

The APs have three cryptographic libraries – Ruckus Access Point SSL Crypto Library (version 5.2.1.3), Ruckus Access Point Kernel Crypto Library (version 5.2.1.3), and Ruckus Access point Radio Crypto Library (version 1.0). The associated CAVP certificates are:

Ruckus Access point Radio Crypto Library (version 1.0):

Requirements	Functions	AP Cert
	Encryption/Decryption	

Requirements	Functions	AP Cert
FCS_COP.1/DataEncryption [WLAN]	**AES CCMP (128 and 256 bits)**	**5312**

Ruckus Access Point SSL Crypto Library (version 5.2.1.3):

Requirements	Functions	AP Cert
	Cryptographic key generation	
FCS_CKM.1	**RSA schemes using cryptographic key sizes of 2048-bits, 3072-bits**	**C2093**
FCS_CKM.1	**ECC schemes using 'NIST curves'** **P-256, P-384, P-521**	**C2093**
	Cryptographic key establishment/distribution	
FCS_CKM.2	**RSA-based key establishment schemes**	**Vendor Affirmed**
FCS_CKM.2	**Elliptic curve-based key establishment schemes**	**C2093**
	Cryptographic key distribution	
FCS_CKM.2/GTK	**AES Key Wrap in EAPOL-Key frame decryption only (as TOE acts as Authenticator only, and not as a supplicant) (128 bits)**	**C2093**
	Encryption/Decryption	
FCS_COP.1/ DataEncryption	**AES CBC and GCM (128 and 256 bits)**	**C2093**
FCS_COP.1/ DataEncryption	**AES CTR (128 and 256 bits)**	**C2093**
	Cryptographic signature services	
FCS_COP.1/SigGen	**RSA Digital Signature Algorithm (rDSA) (modulus 2048)**	**C2093**
FCS_COP.1/SigGen	**Elliptic Curve Digital Signature Algorithm (ECDSA) with an elliptical**	**C2093**

Requirements	Functions	AP Cert
	curve size of 256, 384, or 521 bits	
	Cryptographic hashing	
FCS_COP.1/Hash	**SHA-1/256/384/512 (digest sizes 160, 256, 384 and 512 bits)**	**C2093**
	Keyed-hash message authentication	
FCS_COP.1/ KeyedHash	**HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (key and output MAC sizes 160, 256, 384 and 512 respectively)**	**C2093**
	Random bit generation	
FCS_RBG_EXT.1	**CTR_DRBG (AES) and Hash_DRBG with HW based noise sources (256 bits)**	**C2093**

Ruckus Access Point Kernel Crypto Library (version 5.2.1.3):

Requirements	Functions	AP Cert
	Cryptographic key generation	
FCS_CKM.1(2) [WLAN]	**WPA2 128-bit cryptographic key derivation**	**C2092** **See WFA certificates below**
	Encryption/Decryption	
FCS_COP.1/ DataEncryption	**AES CBC, GCM (128 and 256 bits)**	**C2092**
	Cryptographic hashing	
FCS_COP.1/Hash	**SHA-1/256/384/512 (digest sizes 160, 256, 384 and 512 bits)**	**C2092**
	Keyed-hash message authentication	
FCS_COP.1/ KeyedHash	**HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 (key and output MAC sizes 160, 256, 384 and 512 respectively)**	**C2092**

KEY Generation/Establishment

For asymmetric keys, the TOE supports RSA schemes using cryptographic key sizes of 2048-bit or greater that meet FIPS PUB 186-4, “Digital Signature Standard (DSS)” ECC schemes that use 'NIST curves' P-256, P-384, P-521 that

meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.4, FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, 'Digital Signature Standard (DSS)', Appendix B.1, FFC safe primes schemes using Diffie-Hellman group 14 that meet RFC 3526, Section 3, WPA2/WPA3 128 bit cryptographic key derivation, and WPA3 192 bit cryptographic key derivation.

The table below identifies the usage for each key establishment scheme supported by the TOE:

Security Function	Communication Type	Key Establishment Scheme
Remote administration via the Controller	TLS/HTTPS	RSA Schemes ECC Schemes FFC Schemes
Remote administration via the Controller; Control/Management channel between the Controller (SZ) and the AP and between the Controller (SZ) and the vSZ-D.	SSH	RSA Schemes ECC Schemes FFC Safe-Primes (DH-14)
Trusted channel for Syslog; Data channel between the Controller and the AP and between the vSZ-D and the AP	IPSec	RSA Schemes ECC Schemes FFC Safe-Primes (DH-14)
Trusted channel for authentication services	RadSec	RSA Schemes ECC Schemes FFC Schemes
Trusted channel for WLAN clients	WPA3/WPA2	WPA3/WPA2 128-bit Key derivation

For TLS connections between a remote administrator and the Controller (SZ/vSZ), the TOE supports DH-3072 or secp384r1 for key establishment.

For all symmetric keys, the TOE supports PRF-384 with 128 keys sizes. In the distributed TOE deployment, AP acts as the authenticator and derives the 802.11 keys. With WPA2/WPA3-enterprise connections via 802.1X, all communications between the AP and wireless client is encapsulated in EAP and all traffic between AP and the controller is secured via SSH. The controller to RADIUS server communication is secured via RADSEC. The TOE supports standard WPA2/WPA3-enterprise with 802.11i where 4 way EAP handshake is between the Authenticator (AP) and the wireless client.

AP sends the EAPOL identity to the wireless client, which responds with a radius access request. Upon successful authentication, radius access accept message is received by the client. A PMK is then generated by the RADIUS server for Authenticator and client after which a PTK is derived. The Authenticator also generates a GTK. If the 4-way handshake fails, the client will not be allowed to access the network or connect to the AP.

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/WPA3 handshake. Third part is TK, which is actually used to encrypt/decrypt communication between both AP and Client.

The Ruckus implementation of PTK generation complies to the following sections of IEEE 802.11-2012:

- Section 4.10.3.2 --> AKM operations with AS (WPA2/WPA3 4-way handshake explaining PTK/GTK transfer)
- Section 11.6.1.3 → Pairwise key hierarchy (PTK derivation using the PRF function)

The Ruckus implementation of GTK generation complies to the following sections of IEEE 802.11-2012:

- Section 4.10.3.2 --> AKM operations with AS (WPA2/WPA3 4-way handshake explaining PTK/GTK transfer)
- Section 11.6.1.4 --> Group key hierarchy (GTK derivation using the PRF function)

When the RADIUS protocol is used between the TOE and the authentication server, the MS-MPPE-Recv-Key attribute (vendor-id = 17; see Section 2.4.3 in IETF RFC 2548-1999 [B30]) is used to transport the PMK to TOE. The GTK is distributed by using AES Key Wrap in an EAPOL-Key frame in accordance with the 802.11-2012 standard for the packet format and timing considerations.

Certification testing performed by the Wi-Fi Alliance demonstrates that the TOE implements the IEEE 802.11-2012 standard correctly. Refer to the Wi-Fi Alliance certificates for compliance, https://www.wi-fi.org/certification.

Device Name	Wi-Fi Alliance Certificate Numbers
R650 (Including R650-WW)	WFA100880
R750 (Including T750SE/T750 Omni and T750-WW)	WFA99977
R850	WFA101708

IPSEC

The TOE supports IPSec communication between the TOE components – in the hardware deployment between the Controller (SZ) and AP and in the virtual deployment between the vSZ-D and the AP. It also supports IPsec for communication to an external syslog server via the Controller (SZ/vSZ). The TOE uses the encapsulating security payload (ESP) to protect the payloads of the traffic. Only IKEv2 is supported for both IPsec implementations.

For IPSec between AP and SZ/vSZ-D, the TOE uses AES-128 with SHA1 and MODP 2048, AES-256 with SHA384 and ECP384. As part of this negotiation, the TOE verifies that the negotiated phase 2 symmetric algorithm key strength is at most as large as the negotiated phase 1 key strength as configured on the TOE and peer via an explicit check. The default time value for Phase 1 SAs is 4 hours, but is configurable from 1 minute to 24 hours. The default time value for Phase 2 SAs is 1 hour, but it is configurable 1 minute to 8 hours.

The Security policy is based on the WLAN configuration - only specific WLAN traffic that the administrator chooses is protected via IPsec in transport mode only between the AP and SZ/vSZ-D. All other traffic including WLANs that are not configured for IPsec is bypassed and transmitted locally from AP. All traffic that does not match the configured network is discarded.

The IPsec tunnel between AP and SZ/vSZ-D supports X.509v3 based authentication. The IKEv2 protocol implements DH Groups 14 (2048-bit MODP) and 20 (384-bit Random ECP). The Administrator selects the DH group. The TOE generates the secret value x used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 224 or 384 bits (for DH Groups 14 and 20, respectively). The nonce generated is 32 bytes long (or 256 bits), thus being over 128 bits in size and larger than half the output size of SHA384, and is generated with the DRBG specified in FCS_RBG_EXT.1.

For the peer authentication using RSA X509 certificates, the TOE validates the following identifier:

- Full distinguished name (DN).

For IPSec between the Controller (SZ/vSZ) and an external syslog server, the TOE uses AES-128, AES-192, AES-256 with HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 and ECP384.

As part of this negotiation, the TOE verifies that the negotiated phase 2 symmetric algorithm key strength is at most as large as the negotiated phase 1 key strength as configured on the TOE and peer via an explicit check. The default time value for Phase 1 SAs is 4 hours, but is configurable from 1 minute to 24 hours. The default time value for Phase

2 SAs is 4 hours, but it is configurable 1 minute to 8 hours. The tunnel between the Controller and the external syslog server supports X.509v3 and PSK based authentication.

The IKEv2 protocol implements DH group 20 (384-bit Random ECP). The secret 'x' generated is 48 bytes long (or 384 bits) and is generated with the DRBG specified in FCS_RBG_EXT.1. The nonce generated is 32 bytes long (or 256 bits), thus being over 128 bits in size and half the output size of SHA512, and is generated with the DRBG specified in FCS_RBG_EXT.1

For the peer authentication using X509 certificates, either ECDSA or RSA, the TOE validates the following identifier:

- Full distinguished name (DN).

Once the IPsec configuration is defined in the Controller, it initiates the tunnel to the external component defined in the controller. All inbound and outbound traffic to/from the audit server is protected by IPsec in tunnel mode only. All other traffic is bypassed. All traffic that does not match the configured network is discarded. When a packet destined for the Audit server is processed by the TOE and it determines it requires IPsec, it uses active SA settings or creates new SAs for initial connections with the IPsec peer.

The TOE supports both bit based and text based keys for Pre-shared keys. A TOE administrator specifies the PSK in the Controller configuration. The PSK includes a combination of upper and lower-case letters, numbers, and supported special characters and must be 44-128 for Hex characters and 8-64 for ASCII.

SSH

The TOE supports SSHv2 for both secure remote administration as well as for communications between TOE components. In the distributed TOE, the AP and vSZ-D are SSH clients which communicate to the SSH Server which is the SmartZone controller (SZ/vSZ) via only public key auth (No password-based authentication). SSH for remote administration to the SmartZone controller support both public key and password-based authentication.

The SSH client implementation (between TOE components) supports the following:

- Encryption Algorithms: aes128-ctr, aes256-ctr and aes256-gcm@openssh.com
- Host Key and Public Key authentication algorithms: ssh-rsa
- Data Integrity MAC algorithms: hmac-sha1, hmac-sha2-256, hmac-sha2-512 and implicit
- Key Exchange Methods: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521

The SSH Server implementation (for both remote administration and between TOE components) supports the following:

- Encryption Algorithms: aes128-ctr, aes256-ctr and aes256-gcm@openssh.com
- Host Key authentication algorithms: ssh-rsa, rsa-sha2-256, rsa-sha2-512, ecdsa-sha2-nistp384
- Public Key authentication algorithms: ssh-rsa, ecdsa-sha2-nistp384
- Data Integrity MAC algorithms: hmac-sha1, hmac-sha2-256, hmac-sha2-512 and implicit
- Key Exchange Methods: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521

Packets larger than 256K bytes are dropped.

The SSH session key will be re-negotiated when either one of the following two conditions is met:

1) The maximum amount of data transmitted over the SSH connection exceeds 1G bytes
2) The maximum amount of connection time exceeds 1 hour.

TLS

The TOE supports TLSC in support of RADSEC and TLSS in support of remote administration via the Web UI using HTTPS. As a TLS client, the TOE conforms only to TLS 1.2(RFC 5246). The TOE supports the ciphersuites defined in Section 5.1.3.15. The TLS session is established only when the server certificate is valid. The following elliptic curves are supported in the client hello - secp256r1, secp384r1, secp521r1.

The reference identifier is configured by the administrator of the TOE. The Controller as the TLS client initiates a RADSEC connection and verifies the presented identifier (FQDN) of the server in the certificate that server presents to it. Once the reference identifier is received, the client tries to initiate the TLS connection to the server. IP address, wild cards and certificate pinning are not supported.

The TLS Server is also provided via the Controller and supports TLS 1.2. It supports the ciphersuites defined in Section 5.1.3.16. The TOE will deny connections from clients that request SSL2.0, SSL3.0, TLS1.0 and TLS1.1. The TOE performs key establishment with ECDH over secp384r1, and DH parameters of size 3072 bits. The TLS Server does not support session resumption based on session IDs or session tickets.

RADSEC

The TOE supports RADIUS over TLS as specified in RFC 6614. The TOE performs the function of a RADSEC client and conducts mutual authentication via X.509v3 certificates. The TOE supports only TLS 1.2 and rejects all other TLS and SSL versions. The TOE supports the ciphersuites defined in Section 5.1.3.15. The TOE will present the supported elliptic curve extensions with the following NIST curves: secp256r1, secp384r1, secp521r1 and the supported group extension ffdhe2048. The TLS ciphersuites and NIST curves are not configurable.

The reference identifier is configured by the administrator of the TOE. The Controller initiates the RADSEC connection and verifies the presented identifier (FQDN) of the server in the SAN field of the certificate that the server presents to it. If the certificate is not valid, the connection is dropped. IP address and wild card are not supported. OCSP is supported to verify the validity of the certificate.

The Cryptographic support function satisfies the following security functional requirements:

- NDcPP22e:FCS_CKM.1: The TOE supports cryptographic key generation for the following schemes: RSA schemes using key sizes of 2048 bits or greater, ECC schemes using NIST curves P-256, P-384, and P-521, FFC schemes using key sizes of 2048 bits or greater, FFC schemes using Diffie-Hellman group 14 and WPA2/WPA3 128 bit cryptographic key derivation.
- WLANAS10:FCS_CKM.1/WPA: See NDcPP22e:FCS_CKM.1
- NDcPP22e:FCS_CKM.2: See NDcPP22e:FCS_CKM.1
- WLANAS10:FCS_CKM.2/GTK: As described above, the TOE supports cryptographic key distribution for 802.11 PMK key reception from an 802.1X authentication server, AES Key Wrap in EAPOL-Key frame and Group Key Handshake
- WLANAS10:FCS_CKM.2/PMK: See WLANAS10:FCS_CKM.2/GTK
- NDcPP22e:FCS_CKM.4: All data is cleared as identified in Section 8
- NDcPP22e:FCS_COP.1/DataEncryption: The TOE performs encryption and decryption using AES in CBC CCMP, CTR, and GCM mode with key sizes of either 128, 192 (CBC and GCM), or 256
- WLANAS10:FCS_COP.1/DataEncryption:): See NDcPP22e:FCS_COP.1/DataEncryption
- The TOE supports cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 with digest sizes 160, 256, 384, and 512.
- NDcPP22e:FCS_COP.1/KeyedHash: The TOE supports keyed-hash message authentication using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 using SHA-1/256/384/512 with 160/256/384/512 bit keys to produce a 160/256/384/512 output MAC,
- NDcPP22e:FCS_COP.1/SigGen: The TOE supports the use of RSA with 2048 bit key sizes and ECDSA signatures with curves P-256, P-384, and P-521 for cryptographic signatures. Digital signatures are used in TLS and SSH communications and on product updates.
- NDcPP22e:FCS_HTTPS_EXT.1: The TOE provides HTTPS (via TLS1.2), as specified in RFC 2818, to provide a secure interface for remote administrative functions.

- NDcPP22e:FCS_IPSEC_EXT.1:FCS_IPSEC_EXT.1: The TOE supports IPsec cryptographic network communication protection (RFC 4868, RFC 4945).
- NDcPP22e:FCS_NTP_EXT.1: The TOE supports protected communication to an NTP server using NTP v4. Authentication is performed using the SHA1 message digest algorithm
- WLANAS10:FCS_RADSEC_EXT.1: The TOE supports RADIUS over TLS as specified in RFC 6614. The TOE performs the function of a RADSEC client and conducts mutual authentication via X.509v3 certificates.
- NDcPP22e:FCS_SSHC_EXT.1/NDcPP22e:FCS_SSHS_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above. SSH is also supported for interaction among the distributed components.
- NDcPP22e:FCS_TLSC_EXT.1: The TOE supports TLS v1.2 for support of RADSEC
- NDcPP22e:FCS_TLSS_EXT.1: The TOE supports TLS/HTTPS web-based secure administrator sessions.

6.4 User data protection

The User data protection function satisfies the following security functional requirements:

- WIDS10:FDP_IFC.1: The TOE provides a security policy to monitor the following:
  - authorized APs and authorized EUDs
  - authorized APs and unauthorized EUDs
  - unauthorized APs and unauthorized EUDs

The details of the security policy can be found in FAU_WID_EXT.1 and FAU_WID_EXT.2.

6.5 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, except to display a message of the day banner. The Controller provides a local console as well as remote administration of the system via secure communication channel (WebGUI via HTTPS and CLI via SSH). The AP and vSZ-D do not support authentication of Security Administrators and there are no unauthenticated services/services supported by these components.

The TOE supports a password enforcement configuration where the minimum password length can be set by an administrator. The default minimum length is 8 and this can set to as high as 64 characters. Passwords can be created using any alphabetic, numeric, and a range of special characters (identified in FIA_PMG_EXT.1).

The Administrator can set a lockout failure count for remote login attempts (the default is 3 attempts). If the count is exceeded, the account gets locked out until an administrator configured time has passed. The local administrator account never gets locked out

The Identification and authentication function satisfies the following security functional requirements:

- WLANAS10:FIA_8021X_EXT.1: See WLANAS10:FCS_CKM.2/GTK and the KEY Generation/Establishment portion of Section 6.3 above.
- NDcPP22e:FIA_AFL.1: The Controller provides remote administration of the system via secure communication channel (WebGUI via HTTPS and CLI via SSH. Unsuccessful attempts beyond an administrator configured limit will result in access being denied until an administrator configured time duration has elapsed. The local system administrator can login into the TOE while remote administrators are blocked.
- NDcPP22e:FIA_PMG_EXT.1: The TOE implements a rich set of password composition constraints as described above.

- WLANAS10:FIA_PSK_EXT.1: The TOE supports use of preshared keys for IPSec, 802.11 WPA2-PSK/ WPA3_SAE SSID (single PSK and dynamic PSK). The TOE accepts both bit based and text based keys for Pre-shared keys. A TOE administrator specifies the PSK in the controller configuration. For IPsec, the PSK includes a combination of upper and lower-case letters, numbers, and supported special characters and must be 44-128 for Hex characters and 8-64 for ASCII. For 802.11 WPA2-PSK/WPA3_SAE SSID text based keys, the TOE accepts 22-63 characters with any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")"). For bit based pre-shared keys, 64 Hex characters must be used. The TOE does not generate bit based keys. Text based/ASCII WPA2/ WPA3_SAE passwords are converted to 256 bit based on HMAC SHA1 and IPSec passwords are converted using PRF.
- WLANAS10:FIA_UAU.6: Upon change of an administrator password by the administrator themselves, the TOE will reauthenticate the administrator.
- NDcPP22e:FIA_UAU.7: The TOE does not echo passwords as they are entered; rather '*' characters are echoed when entering password.
- NDcPP22e:FIA_UAU_EXT.2: The TOE requires all administrators of the system to login via credentials (username & password) before granting access to the system. CLI via SSH, WebUI via HTTPS methods are allowed on the Controller for a remote administrator and local console access is allowed to the Controller via authentication as well. Once an administrator tries to access the system, a login screen is presented where the administrator inputs the credentials. Access to the system is denied if the authentication does not succeed or is not performed.
- NDcPP22e:FIA_UIA_EXT.1: The TOE requires all administrators of the system to login via credentials (username & password) before granting access to the system. When the login screen is presented, the TOE presents a customized banner. Administrators can manage the TOE components via the Controller.
- NDcPP22e:FIA_X509_EXT.1/ITT: The TOE provides X.509 v3 based authentication between the components in accordance to RFC 5280. The TOE components perform certificate validation when establishing an IPsec session which includes verifying the extendedKeyUsage field in the certificates that are exchanged. The TOE rejects the connection if certificate validation fails. The TOE does not support revocation checking for certificate validation between the distributed components.
- NDcPP22e:FIA_X509_EXT.1/Rev: The TOE provides X.509v3 based authentication for communications with external components via IPSec for the audit server and RADSEC in accordance to RFC 5280. The Controller performs the certificate validation when it tries to join an external component. The Controller verifies the extendedKeyUsage field. The TOE supports OCSP to verify the validity of the certificates presented by the external component, including the leaf cert and any intermediate certs received, regardless of the cert chain length. Administrators can upload the CA chain and map which certificates to use for different external connections. The TOE rejects the connection if the certificate validation fails.
- NDcPP22e:FIA_X509_EXT.2: Certificates are checked and if found not valid are not accepted or if the OCSP server cannot be contacted for validity checks, then the certificate is not accepted.
- NDcPP22e:FIA_X509_EXT.3: The TOE supports the certificate request message generation as specified by RFC 2986 and provides the following information – public key, Common Name and Country.

6.6 Security management

The TOE provides the ability to perform administrative functions as an authorized user. All authorized users are granted the Administrator role. Administrators can control the TOE components (Controller (SZ/vSZ), vSZ-D and AP) via the Controller. Only authenticated administrators are allowed access to the TOE to perform administrative functions via WebUI (HTTPS), CLI (SSH) and Local Console. All security functions are available through all interfaces.

The following administrative functions are supported:

- 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 manage the cryptographic keys,
- Ability to configure the cryptographic functionality,
- Ability to configure the lifetime for IPsec SAs;
- Ability to configure the interaction between TOE components;
- Ability to set the time which is used for time-stamps;
- Ability to configure NTP;
- 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,
- Configure approval/denial of AP and vSZ-D to communicate/join the controller
- 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
- Define an inventory of authorized APs based on [MAC addresses]
- Define an inventory of authorized EUDs based on MAC addresses
- Define rules for monitoring and alerting on the wireless traffic
- Define authorized SSID(s)
- Define authorized WLAN authentication schemes
- Define authorized WLAN encryption schemes
- disable transmission of data by wireless sensor,
- Define attack signatures,
- Define rules for overwriting previous packet captures,
- Define the amount of time sensor monitors a specific channel

The Security management function satisfies the following security functional requirements:

- NDcPP22e:FMT_MOF.1/ManualUpdate: Only the authorized administrator can update the TOE.

- NDcPP22e:FMT_MTD.1/CoreData: Security management is restricted to administrators.
- NDcPP22e:FMT_MTD.1/CryptoKeys: Only the authorized administrator can perform operations on cryptographic keys.
- NDcPP22e:FMT_SMF.1: The TOE provides administrative local, and remote interfaces via WebUI (HTTPS), CLI (SSH) to perform the functions identified above.
- WLANAS10:FMT_SMF.1/AccessSystem: : See NDcPP22e:FMT_SMF.1.
- WIDS10:FMT_SMF.1/WIDS: : See NDcPP22e:FMT_SMF.1.
- NDcPP22e:FMT_SMR.2: The TOE maintains the administrative user role.
- WLANAS10:FMT_SMR_EXT.1: By default, the TOE cannot be administered remotely from a wireless device.

6.7 Protection of the TSF

The TOE is designed to protect critical security parameters. The TOE provides no mechanism to read or disclose private keys, preshared keys, passwords or symmetric keys stored in TOE. Keys are stored in internal storage. Passwords are stored in non-plaintext form and are obscured. Passwords are encrypted in storage.

The TOE provides reliable timestamps by synchronizing time via NTP securely. The timestamps are used in audit records, certificate validation, session monitoring activity and Wireless client access management.

When the TOE boots up, each component of the TOE performs POST (Power On Self-Test) for all cryptographic modules. The tests include:

- AES Known Answer Test
- SHA Known Answer Test
- HMAC Known Answer Test
- CCM Known Answer Test
- GCM Known Answer Test
- DRBG Known Answer Test
- Software Integrity test (RSA with SHA384)
- CMAC Known Answer Test
- RSA Known Answer Test
- ECDSA Pairwise Consistency Test
- ECC CDH shared secret computation

When any one of the known answer tests fails, the system will enter the quarantine state. Upon critical failure, the TOE component either goes into a quarantine state and can be recovered only by a security administrator or it reboots and disables access to its interfaces.

The TOE provides the ability to query a currently running firmware version via both the WebUI and the CLI after logging in. The TOE also provides the ability to obtain and apply a new software version via the Web UI. The new software update is first uploaded and then activated later when the administrator selects the upgrade option. The Controller in turn will upgrade the APs and vSZ-D once it has applied the software on itself securely via SSH. All components of the TOE are updated via the controller. All controller, AP and vSZ-D updates are verified via digital signatures. Software installation will fail if the signature verification fails. All software updates are hosted on Ruckus support portal and can be downloaded securely via HTTPS after authenticating to the server

The Protection of the TSF function satisfies the following security functional requirements:

- NDcPP22e:FPT_APW_EXT.1: The TOE does not offer any functions that will disclose to any user a plain text password.
- WLANAS10:FPT_FLS.1: Upon critical failure, the TOE component either goes into a quarantine state and can be recovered only by a security administrator or it reboots and disables access to its interfaces.
- NDcPP22e:FPT_ITT.1: The TOE has 3 components, a Controller, an AP, and in virtual deployments, a vSZ-D. All management communications between the Controller and AP and between the controller and vSZ-D are secured via SSH. Data traffic between AP and vSZ-D or Controller is secured via IPsec. The distributed communications are encrypted the same regardless of the AP being in a wired or mesh configuration. Section 6.2 describes the protocols and their options in the evaluated configuration.
- NDcPP22e:FPT_SKP_EXT.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- NDcPP22e:FPT_STM_EXT.1: The TOE allows system administrators to set the time used by the TOE using NTP. This time is used by the TOE for the activities listed above.
- NDcPP22e:FPT_TST_EXT.1: The TOE includes a number of power-on diagnostics that will serve to ensure the TOE is functioning properly. These tests include cryptographic known answer tests and software integrity tests.
- WLANAS10:FPT_TST_EXT.1: See NDcPP22e:FPT_TST_EXT.1
- NDcPP22e:FPT_TUD_EXT.1: The TOE provides function to query the version and upgrade the software in the TOE components. When installing updated software, digital signatures are used to authenticate the update to ensure it is the update intended and originated by Ruckus.

6.8 TOE access

The TOE security administrator can configure the session inactivity timeout which terminates the sessions of administrators once the session inactivity timeout is reached for both local and remote interactive sessions. Administrators also have the ability to terminate their own session by clicking logout on the WebUI and typing exit on the CLI.

The TOE provides the ability for administrators to configure a login banner which will be visible to users when they try to access the controller prior to log in via WebUI or CLI.

The TOE provides the ability to deny establishment of a wireless client session based on TOE interface, time, and day.

The TOE access function satisfies the following security functional requirements:

- NDcPP22e:FTA_SSL.3: The TOE terminates remote sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_SSL.4: The TOE provides the function to logout (or terminate) the both local and remote user sessions as directed by the user.
- NDcPP22e:FTA_SSL_EXT.1: The TOE terminates local sessions that have been inactive for an administrator-configured period of time.
- NDcPP22e:FTA_TAB.1: The TOE can be configured to display administrator-defined advisory banners when administrators successfully establish interactive sessions with the TOE.
- WLANAS10:FTA_TSE.1: The TOE can deny a wireless client session based on TOE interface, time, and day.

6.9 Trusted path/channels

The TOE provides secure communication channels for external communications and remote administration. The Controller uses secure channels to communicate to external components.

- Audit server via IPSec (TOE can acts as initiator)
- RADIUS via RADSEC (TOE acts as TLS client)
- Wireless client connecting to TOE AP via WPA3 or WPA2

The Controller also supports all remote administrative functions via secure channels - WebUI (HTTPS) and CLI (SSH).

The TOE supports distributed TOE communication. The SmartZone controller is configured first, then other components, AP and vSZ-D are configured to join to the controller by assigning the IP address of the controller. After approval of the join request those appliances are managed by the SmartZone Controller. This initial registration is performed over a dedicated channel so confidentiality is not required. After registration, confidentiality is enforced as SSH is used for all management of the distributed TOE components (AP and vSZ-D) by the SmartZone Controller and IPSec is used for the data tunnel. If the initial joining of any component (AP or vSZ-D) to the SmartZone controller fails, no communication between the components is possible, other than an attempt at rejoining. In this case the admin should verify the registration steps were performed correctly and the network setup is correct.

The Trusted path/channels function satisfies the following security functional requirements:

- NDcPP22e/WIDS10:FTP_ITC.1: The TOE uses secure communications channels for all external communications as identified above.
- WLANAS10:FTP_ITC.1: For wireless users, IEEE 802.11-2012 (WPA2) and IEEE 802.1X are used to provide a trusted channel between the TOE and authentication servers and audit servers.
- WLANAS10:FTP_ITC.1/Client: For wireless users, WPA3-Enterprise, WPA2-Enterprise, WPA3-SAE and WPA2-PSK as defined by IEEE 802.11-2020 are used to provide a trusted channel between the TOE and WLAN clients. If the client attempts to use another security type to establish a connection, the authentication attempt will be rejected.
- NDcPP22e:FTP_TRP.1/Admin: The TOE uses SSH, TLS/HTTPS to provide a trusted communication path between itself and 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 detection of modification of the communicated data.
- NDcPP22e:FTP_TRP.1/Join: The TOE uses a dedicated channel to provide a trusted communication path between distributed TOE components that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification.

7. Requirement Allocation

This section provides a mapping of the distributed TOE components to the SFRs in this ST. This TOE is a distributed TOE consistent with Use Case 3 as defined in the NDcPP22e. The following table presents the required mapping.

Requirement	Distributed TOE SFR Allocation	Distributed TOE Audit Event Allocation
WIDS10:FAU_ARP.1	Controller, AP	AP
WIDS10:FAU_ARP_EXT.1	Controller	No event required
NDcPP22e/WLANAS10:FAU_GEN.1	All	All
WIDS10:FAU_GEN.1/WIDS	All	All
NDcPP22e:FAU_GEN.2	All	No event required
NDcPP22e:FAU_GEN_EXT.1	All	No event required
NDcPP22e\WIDS10:FAU_STG_EXT.1	All	No event required
WIDS10:FAU_IDS_EXT.1	Controller	No event required
WIDS10:FAU_INV_EXT.1	Controller	Controller
WIDS10:FAU_INV_EXT.2	Controller	No event required
WIDS10:FAU_INV_EXT.3	Controller	Controller
WIDS10:FAU_RPT_EXT.1	Controller	No event required
WIDS10:FAU_SAA.1	Controller, AP	No event required
NDcPP22e/WISD10:FAU_STG_EXT.4	All	No event required
NDcPP22e:FAU_STG_EXT.5	All	No event required
WIDS10:FAU_WID_EXT.1	Controller, AP	AP
WIDS10:FAU_WID_EXT.2	Controller, AP	AP
NDcPP22e/WIDS10:FCO_CPC_EXT.1	All	All
NDcPP22e:FCS_CKM.1	All	No event required
WLANAS10:FCS_CKM.1/WPA	Controller, AP	No event required
NDcPP22e:FCS_CKM.2	All	No event required
WLANAS10:FCS_CKM.2/GTK	Controller, AP	No event required
WLANAS10:FCS_CKM.2/PMK	Controller, AP	No event required
NDcPP22e:FCS_CKM.4(1) AP	AP	No event required
NDcPP22e:FCS_CKM.4(2) SZ, vSZ-D	Controller, vSZ-D	No event required
WLANAS10:FCS_COP.1/DataEncryption	Controller, AP	No event required
NDcPP22e:FCS_COP.1/DataEncryption	All	No event required
NDcPP22e:FCS_COP.1/Hash	All	No event required
NDcPP22e:FCS_COP.1/KeyedHash	All	No event required
NDcPP22e:FCS_COP.1/SigGen	All	No event required
NDcPP22e:FCS_HTTPS_EXT.1	Controller	Controller
NDcPP22e:FCS_IPSEC_EXT.1	All	Controller, AP, vSZ-D
NDcPP22e:FCS_NTP_EXT.1	Controller	Controller
WLANAS10:FCS_RADSEC_EXT.1	Controller	No event required
NDcPP22e:FCS_RBG_EXT.1	All	No event required
NDcPP22e:FCS_SSHC_EXT.1	AP, vSZ-D	AP, vSZ-D
NDcPP22e:FCS_SSHS_EXT.1	Controller	Controller
NDcPP22e:FCS_TLSC_EXT.1	Controller	Controller
NDcPP22e:FCS_TLSS_EXT.1	Controller	Controller
WIDS10:FDP_IFC.1	All	No event required
WLANAS10:FIA_8021X_EXT.1	Controller, AP	AP
NDcPP22e:FIA_AFL.1	Controller	Controller
NDcPP22e:FIA_PMG_EXT.1	Controller	No event required
WLANAS10:FIA_PSK_EXT.1	Controller	No event required

WLANAS10:FIA_UAU.6	Controller	Controller
NDcPP22e:FIA_UAU.7	Controller	No event required
NDcPP22e:FIA_UAU_EXT.2	Controller	Controller
NDcPP22e:FIA_UIA_EXT.1	Controller	Controller
NDcPP22e:FIA_X509_EXT.1/ITT	All	All
NDcPP22e:FIA_X509_EXT.1/Rev	Controller	Controller
NDcPP22e:FIA_X509_EXT.2	All	No event required
NDcPP22e:FIA_X509_EXT.3	All	No event required
NDcPP22e:FMT_MOF.1/ManualUpdate	All	All
NDcPP22e:FMT_MTD.1/CoreData	All	No event required
NDcPP22e:FMT_SMF.1	Controller	Controller
WLANAS:FMT_SMF.1/AccessSystem	Controller	No event required
WIDS10:FMT_SMF.1/WIDS	Controller	No event required
WLANAS10:FMT_SMR_EXT.1	Controller	No event required
NDcPP22e:FMT_SMR.2	Controller	No event required
NDcPP22e:FPT_APW_EXT.1	All	No event required
WLANAS10:FPT_FLS.1	All	All
NDcPP22e:FPT_ITT.1	All	All
WLANAS10:FPT_ITT.1	All	All
NDcPP22e:FPT_SKP_EXT.1	All	No event required
NDcPP22e:FPT_STM_EXT.1	All	All
NDcPP22e:FPT_TST_EXT.1	All	No event required
WLANAS10:FPT_TST_EXT.1	All	All
NDcPP22e:FPT_TUD_EXT.1	All	All
NDcPP22e:FTA_SSL.3	Controller	Controller
NDcPP22e:FTA_SSL.4	Controller	Controller
NDcPP22e:FTA_SSL_EXT.1	Controller	Controller
NDcPP22e:FTA_TAB.1	Controller	No event required
WLANAS10:FTA_TSE.1	AP	AP
NDcPP22e:FTP_ITC.1	Controller	Controller
WLANAS10:FTP_ITC.1	Controller, AP	Controller, AP
WLANAS10:FTP_ITC.1/Client	Controller, AP	Controller, AP
NDcPP22e:FTP_TRP.1/Admin	Controller	Controller
NDcPP22e:FTP_TRP.1/Join	All	All

8. Key Clearing

This section provides an identification of each secret key, private key and CSP and identifies when and how it is cleared.

Zeroization is performed when setting the Controller out of or into a FIPS-Approved mode of operation using the "fips enable/disable" command. This is required so that keys and other sensitive information established in one mode cannot be used in another. Other than changing the FIPS mode by using the fips enable/disable command on the Controller, zeroization can happen if the CLI command "fips zeroization" is issued on vSZ-D or "zeroize-all csp" command on AP (via controller).

For secure connections, keys can be stored in RAM. Keys stored in RAM are destroyed with a power cycle/reboot on all TOE components. On the SZ and vSZ-D, when the connection (session) is terminated, the keys are erased by writing zeros in the corresponding RAM location. On the AP, when the session is terminated, the keys are erased with a pseudo random pattern written in the corresponding RAM location. When keys are stored in Flash and zeroized via command, the keys are erased in a similar way to the keys found in RAM. On the SZ and vSZ-D, the keys are erased by writing zeros in the corresponding Flash location. On the AP, the keys are erased with a pseudo random pattern written in the corresponding Flash location. This is represented by session termination in the table below.

Name	Description	Type	TOE Component	Storage	Zeroize
TLS Server RSA Private Key	RSA key used to sign server certificate	RSA-3072 Private Key	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS Server RSA Public Key	RSA public key signed as a server certificate	RSA-3072 Public Key	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS Client RSA Private Key	RSA key used to establish a TLS v1.2 session	RSA 2048 – n bits; size dependent on cert. loaded into the module	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS Client RSA Public Key	RSA public key signed as a client certificate	RSA 2048 – n bits; size dependent on cert. loaded into the module	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS Pre-Master Secret	256-bit (ECDH) or 2048-bit (DH) secret value used to establish the TLS Master Secret	TLS key precursor	Controller	RAM	Power cycle Session termination
TLS Master Secret	384-bit secret value used to establish the TLS Encryption Keys	TLS key precursor	Controller	RAM	Power cycle

Name	Description	Type	TOE Component	Storage	Zeroize
	and TLS Authentication Keys				Session termination
TLS DH/ ECDH Host Private Key	Ephemeral DH or ECDH private key used to establish the TLS Pre-Master Secret	DHE: 3072, ECDHE: secp384r1	Controller	RAM	Power cycle fips enable/disable command
TLS DH/ ECDH Host Public Key	Ephemeral DH or ECDH public key sent to the TLS client to establish the TLS Pre-Master Secret	DHE: 3072, ECDHE: secp384r1	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS DH/ ECDH Client Public Key	Ephemeral DH or ECDH public key used to establish the TLS Pre-Master Secret	DHE: 3072, ECDHE: secp384r1	Controller	RAM, Flash	Power cycle (RAM) fips enable/disable command
TLS Encryption Keys	AES keys used to encrypt TLS session data	AES-CBC-128 or AES-CBC-256 or AES-GCM-128 or AES-GCM-256	Controller	RAM	Power cycle Session termination
TLS Authentication Keys	HMAC keys used to authentication TLS session data	HMAC-SHA1 HMAC-SHA256 HMAC-SHA384	Controller	RAM	Power cycle Session termination
Random Number Generation	Entropy Input for the SP800-90A CTR_DRBG	DRBG Seed material	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
DRBG Internal States	Internal State of SP800-90A CTR_DRBG	SP800-90A DRBG State	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)

Name	Description	Type	TOE Component	Storage	Zeroize
Random Number Generation	Entropy Input for Hash_DRBG	DRBG Seed material	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
User Password	Password used to authenticate the User (at least 8 characters)	Authentication data	Controller	AES encrypted (using User Password and UID as the key) and encoded in Flash, RAM	Power cycle (RAM) fips enable/disable command
Enable Password	Password used by the Crypto Officer to enable the CLI(at least 8 characters)	Authentication data	Controller	SHA512 hashed in Flash	fips enable/disable command
Crypto Officer Password	Password used to authenticate the Crypto Officer (at least 8 characters)	Authentication data	Controller	AES encrypted (using User Password and UID as the key) and encoded in Flash	fips enable/disable command
SSHv2 Host RSA/ ECDSA Private Key	Used to sign the SSHv2 Host RSA/ ECDSA Public Key when the module is acting as an SSH host, or the SSHv2 Client RSA Public Key when the module is acting as an SSH client	RSA-2048 ECDSA P-256, P-384, P-521	All	RAM, Flash	Power cycle (RAM) Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)

Name	Description	Type	TOE Component	Storage	Zeroize
SSHv2 Host RSA/ ECDSA Public Key	Used to authenticate SSHv2 server to client	RSA-3072 ECDSA P-256, P-384, P-521 (remote administration only)	All	RAM, Flash	Power cycle (RAM) Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
SSHv2 Client RSA/ ECDSA Public Key	Used to authenticate SSHv2 server to client	RSA-2048 or ECDSA P-256, P-384, P-521 size dependent on the certificate loaded into the module (remote administration only)	All	RAM, Flash	Power cycle (RAM) Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
SSHv2 DH/ ECDH Private Key	DH or ECDH private key used to derive SSH Session and Authentication Keys	DHE: 2048, ECDHE: P-256/384/521	All	RAM	Power cycle Session termination
SSHv2 Host DH/ ECDH Public Keys	Key exchange keys	DHE: 2048, ECDHE: P-256/384/521	All	RAM	Power cycle Session termination
SSHv2 Client DH/ ECDH Public Keys	Key exchange keys	DHE: 2048, ECDHE: P-256/384/521	All	RAM	Power cycle Session termination
SSHv2 Session Keys	AES encryption key used to secure SSHv2	AES-128-CTR or AES-256-CTR or AES-GCM@openssh.com Key	All	RAM	Power cycle Session termination
SSHv2 Authentication Key	Session authentication key used to authenticate and provide integrity of SSHv2 session	HMAC-SHA-1 or HMAC-SHA-256 or HMAC-SHA-512	All	RAM	Power cycle Session termination
SSHv2 KDF Internal State	Used to generate Host encryption and authentication key	KDF	All	RAM	Power cycle

Name	Description	Type	TOE Component	Storage	Zeroize
					Session termination Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
IKEv2/ IPsec Encryption Key	AES keys used to encrypt IKE/ IPsec session data	AES-CBC-128 AES-CBC-256 AES-CBC-192 (Controller to external syslog only)	All	RAM	Power cycle Session termination
IKEv2/ IPsec Authentication Keys	Session authentication key used to authenticate and provide integrity of IKE/ IPsec session	HMAC-SHA-1 HMAC-SHA-256 (Controller to external syslog only) HMAC-SHA-384 HMAC-SHA-512 (Controller to external syslog only)	All	RAM	Power cycle Session termination
IKEv2/ IPsec ECDH Private Key	Used to establish the secret keying material for IKE and IPsec	Group-20 (384-bit Random ECP) Group-14 (2048-bit MODP) (ITT only)	All	RAM	Power cycle Session termination
IKEv2/ IPsec Host ECDH Public Key	Used to establish the secret keying material for IKE and IPsec	Group-20 (384-bit Random ECP) Group-14 (2048-bit MODP) (ITT only)	All	RAM	Power cycle Session termination
IKEv2/ IPsec Client ECDH Public Key	Used to establish the secret keying material for IKE and IPsec	Group-20 (384-bit Random ECP) Group-14 (2048-bit MODP) (ITT only)	All	RAM	Power cycle Session termination
IKEv2/ IPsec Pre-Shared Key	Authenticate the peers to each other	8 char. Minimum Pre-Shared Key	All	Flash, RAM	Power cycle (RAM) Zeroize commands: -fips enable/disable (Controller)

Name	Description	Type	TOE Component	Storage	Zeroize
					-fips zeroization (vSZ-D) -zeroize-all csp (AP)
IKEv2/ IPsec RSA/ ECDSA Private Key	RSA or ECDSA private key used during the IKE/ IPsec handshake to sign the host certificate	RSA-3072 ECDSA P-384 private key (Controller to syslog only)	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
IKEv2/ IPsec Host RSA/ ECDSA Public Key	RSA or ECDSA public key signed as a host certificate	RSA-3072 ECDSA P-384 public key (Controller to syslog only)	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
IKEv2/ IPsec Client RSA/ ECDSA Public Key	RSA or ECDSA public key signed as a client certificate	RSA-3072 ECDSA P-384 public key (Controller to syslog only)	All	RAM	Power cycle Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
Firmware Upgrade Key	RSA key used to sign and verified the integrity of firmware.	RSA-4096 Public Key	All	Temporary file during firmware upgrade	Zeroized after verification of image
NTP Key	Authenticate with NTP server	Authenticate with sha-1 key Type	Controller	RAM, Flash.	Power cycle (RAM) fips enable/disable command

Name	Description	Type	TOE Component	Storage	Zeroize
RADIUS Secret	Authenticate with external radius server	Characters	Controller	RAM	Power cycle Session termination Zeroize commands: -fips enable/disable (Controller) -fips zeroization (vSZ-D) -zeroize-all csp (AP)
PMK	Used to derive 802.11i Pairwise Transient Key(PTK)	802.11i Pairwise Master Key(PMK)	AP	RAM	Power cycle Session termination zeroize-all csp command
PTK	All session encryption/decryption keys are derived from the PTK	802.11i Pairwise Transient Key(PTK)	AP	RAM	Power cycle Session termination zeroize-all csp command
EAPOL Encryption Key	Used for 802.11i message encryption	802.11i EAPOL Encryption Key	AP	RAM	Power cycle Session termination zeroize-all csp command
GMK	Used to derive Group Transient Key(GTK)	802.11i Group Master Key(GMK)	AP	RAM	Power cycle Session termination zeroize-all csp command
GTK	Used to derive multicast cryptographic keys	Used to derive Group Transient Key(GTK)	AP	RAM	Power cycle Session termination zeroize-all csp command

Name	Description	Type	TOE Component	Storage	Zeroize
Group AES-CCM Data Encryption key	Used to protect multicast message confidentiality and integrity (AES-CCM)	802.11i Group AES-CCM Data Encryption/MIC Key	AP	RAM	Power cycle Session termination zeroize-all csp command
AES-CCM session key	Used for 802.11i packet encryption	802.11i AES-CCM session key	AP	RAM	Power cycle Session termination zeroize-all csp command
WPA3/WPA2 PSK	Used for client authentication	WPA3/WPA2 PSK	AP	RAM, Flash	Power cycle (RAM) zeroize-all csp command