National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Network Devices, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems

Version 1.0

05 April 2023

Report Number: CCEVS-VR-PP-0089
Dated: 27 November 2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Network Devices, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems, Version 1.0 (CFG_NDcPP-WIDS-WLANAS_V1.0). This Protection Profile (PP)-Configuration defines how to evaluate a TOE that claims conformance to the collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E) Base-PP, the PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS) (MOD_WIDS_V1.0), and the PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLANAS_V1.0). It presents a summary of the CFG_NDcPP-WIDS-WLANAS_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the CFG_NDcPP-WIDS-WLANAS_V1.0 and the CPP_ND_V2.2E Base-PP, MOD_WIDS_V1.0, and MOD_WLANAS_V1.0, contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 (Ruckus SmartZone).

This evaluation addressed the base security functional requirements (SFRs) of the CPP_ND_V2.2E Base-PP, MOD_WIDS_V1.0, and MOD_WLANAS_V1.0 as part of CFG_NDcPP-WIDS-WLANAS_V1.0. The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Modules as part of the completion of this VR, to confirm they met the claimed APE and ACE requirements.

The evaluation determined the CFG_NDcPP-WIDS-WLANAS_V1.0 is both Common Criteria Part 2 extended and Part 3 conformant. A NIAP approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and Modules identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from CPP_ND_V2.2E, MOD_WIDS_V1.0, and MOD_WLANAS_V1.0; completion of the ASE workunits satisfied the APE workunits for CPP_ND_V2.2E and the ACE workunits for the PP-Modules, but only for the materials defined in these PP-Modules, and only when the PP-Modules are in the defined PP-Configuration.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against PPs and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or PP-Modules. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Modules with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_NDcPP-WIDS-WLANAS_V1.0, CPP_ND_V2.2E, MOD_WIDS_V1.0, and MOD_WLANAS_V1.0 was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Ruckus SmartZone, performed by Gossamer Security Solutions, Inc. in Columbia, Maryland.

This evaluation addressed the base requirements of MOD_WIDS_V1.0, and MOD_WLANAS_V1.0 as part of CFG_NDcPP-WIDS-WLANAS_V1.0.

MOD_WIDS_V1.0 and MOD_WLANAS_V1.0 contain a set of base requirements that all conformant STs must include, and additionally contain optional, selection-based, and objective requirements. Optional requirements may or may not be included within the scope of the evaluation, depending on whether the vendor provides that functionality within the tested product and chooses to include it inside the TOE boundary. Selection-based requirements are those that must be included based on the selections made in other requirements and the abilities of the TOE. Objective requirements are not currently prescribed but are expected to be included in future versions.

The VR author evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ workunits performed against the PP-Modules. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_NDcPP-WIDS-WLANAS_V1.0 were evaluated.

The following identifies the Base-PP and PP-Modules in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these PP-Modules.

PP-Configuration	PP-Configuration for Network Devices, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 2023-04-05
Base-PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020
Modules in PP-Configuration	PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 2020-09-30 PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 2022-03-31
ST (Base)	Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target, Version 0.6, 09/18/2023

Assurance Activity Report (Base)	Assurance Activity Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3, Version 0.4, 09/18/2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Conformant
CCTL	Gossamer Security Solutions, Inc. Columbia, MD

3 CFG_NDcPP-WIDS-WLANAS_V1.0 Description

CFG_NDcPP-WIDS-WLANAS_V1.0 is a PP-Configuration that combines the following:

- collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
- PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0 (MOD_WIDS_V1.0)
- PP Module for Wireless Local Area Network (WLAN) Access System, Version 1.0 (MOD_WLANAS_V1.0)

This PP-Configuration defines a baseline set of SFRs for WIDS/WIPS and WLAN Access Systems applications (defined in CPP_ND_V2.2E) that are bundled with agent applications to enforce configured policies on WIDS/WIPS (defined in MOD_WIDS_V1.0) and WLAN Access Systems (defined in MOD_WLANAS_V1.0).

A conformant WIDS/WIPS is a product that can monitor, collect, inspect, and analyze real-time network traffic and alert the administrator of policy violations. WIPS functionality is not required to conform to this PP-Module, and it is optional for the TOE to have the additional ability to react in real-time to potentially malicious wireless (IEEE 802.11) network traffic.

A compliant WLAN AS is a system composed of hardware and software that is connected to a network and has an infrastructure role in the overall enterprise network. A WLAN AS establishes a secure wireless (IEEE 802.11) link that provides an authenticated and encrypted path to an enterprise network and thereby decreases the risk of exposure of information transiting “over-the-air.”

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_NDcPP-WIDS-WLANAS_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From CPP_ND_V2.2E	
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

Assumption Name	Assumption Definition
A.RESIDUAL_INFORMATION	The Administrator must ensure 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.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.
A.VS_ISOLATION (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
From MOD_WIDS_V1.0	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.
A.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.
These assumptions are made on the Operational Environment to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an Operational Environment that does not meet these assumptions, the TOE may no longer be able to provide all its security functionality.	

Assumption Name	Assumption Definition
From MOD_WLANAS_V1.0	
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.
These assumptions are made on the OE to be able to ensure that the security functionality specified in the PP-Module can be provided by the TOE. If the TOE is placed in an OE that does not meet these assumptions, the TOE may no longer be able to provide all its security functionality. All assumptions for the OE of the Base-PP also apply to this PP-Module. A.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_NDcPP-WIDS-WLANAS_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From CPP_ND_V2.2E	
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

Threat Name	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
From MOD_WIDS_V1.0	
T.DISRUPTION	Attacks against the WLAN infrastructure might lead to denial of service (DoS) attacks within a protected WLAN. A wireless DoS may occur in two ways: at the physical layer through RF Jamming, or at the data link layer through packet injection.
T.UNAUTHORIZED_ACCESS	An attacker may attempt to gain unauthorized access to a network, endpoints, or services, by methods such as impersonation of an authorized AP to get an EUD to connect to the unauthorized AP If malicious external APs or EUDs are able to communicate with APs or EUDs on the protected WLAN, then those devices may be susceptible to the unauthorized disclosure of information.
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	A malicious actor may take advantage of unintended/unauthorized disclosure of sensitive information on a protected WLAN, such as sending unencrypted sensitive data, without detection. A malicious actor may also force the modification or disclosure of data in transit between distributed components of a WIDS to impede or gain visibility into its data collection capabilities.
From MOD_WLANAS_V1.0	
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external

Threat Name	Threat Definition
	devices are able to communicate with devices on the protected network or if devices on the protected network can establish communications with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to be only accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of nonexistent or insufficient WLAN data encryption that exposes the WLAN data in transit to rogue elements), then those internal devices may be susceptible to the unauthorized disclosure of information.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the wireless network and send the packets at a later time, possibly unknown by the intended receiver.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TOE Security Functionality (TSF).

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_NDcPP-WIDS-WLANAS_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From CPP_ND_V2.2E	
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
From MOD_WIDS_V1.0	
P.ANALYZE	Analytical processes and information to derive conclusions about potential intrusions must be applied to WIDS data and appropriate response actions taken.
From MOD_WLANAS_V1.0	
No additional OSPs defined in the MOD_WLANAS_V1.0	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_NDcPP-WIDS-WLANAS_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From CPP_ND_V2.2E	
No security objectives for the TOE defined in CPP_ND_V2.2E.	
From MOD_WIDS_V1.0	
O.SYSTEM_MONITORING	To be able to analyze and react to potential network policy violations, the WIDS must be able to collect and store essential data elements of network traffic on monitored networks. A conformant TOE may also implement a self-protection mechanism to ensure that undetected network policy violations cannot occur when a sensor is unavailable.
O.TOE_ADMINISTRATION	To address the threat of unauthorized administrator access that is defined in the Base-PP, conformant TOEs will provide the functions necessary for an administrator to configure the WIDS capabilities of the TOE. A conformant TOE may also implement a self-protection mechanism to ensure that a TSF failure cannot be used as a way to modify the TOE's configuration without authorization.
O.TRUSTED_COMMUNICATIONS	To further address the threat of untrusted communications channels that is defined in the Base-PP, conformant TOEs will provide trusted communications between distributed components if any exist.
O.WIDS_ANALYZE	The WIDS must be able to analyze collected or observed WLAN activity on monitored network to identify potential violations of approved WLAN policies, unauthorized connections involving internal WLAN devices, and non-secure communications.
O.WIDS_REACT	The TOE must be able to react, as configured by the administrators, to configured policy violations or other potential malicious activity.
From MOD_WLANAS_V1.0	
O.AUTHENTICATION	The TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE will provide means to encrypt and decrypt data to maintain confidentiality and allow for detection of modification of TSF data that is transmitted outside the TOE.
O.FAIL_SECURE	Upon a self-test failure, the TOE will shut down to ensure that data cannot be passed without adhering to the TOE’s security policies
O.SYSTEM_MONITORING	The TOE will provide a means to audit events specific to WLAN functionality and security.
O.TOE_ADMINISTRATION	The TOE will provide the functions necessary to address failed authentication attempts by a remote administrator.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_NDcPP-WIDS-WLANAS_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From CPP_ND_V2.2E	
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.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.TRUSTED_ADMIN	Security 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

Environmental Security Objective	Environmental Security Objective Definition
	• 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.
From MOD_WIDS_V1.0	
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.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.
From MOD_WLANAS_V1.0	
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.
All objectives for the OE of the Base-PP also apply to this PP-Module. OE.NO_THRU_TRAFFIC_PROTECTION is still operative, but only for the interfaces in the TOE that are defined by the Base-PP and not the PP-Module.	

5 Functional Requirements

As indicated above, CFG_NDcPP-WIDS-WLANAS_V1.0 includes CPP_ND_V2.2E, MOD_WIDS_V1.0, and MOD_WLANAS_V1.0.

Requirements in the MOD_WIDS_V1.0 and MOD_WLANAS_V1.0 are comprised of modified Base-PP, "base," and additional requirements that are optional (including strictly optional), selection-based, or objective.

Table 6 defines the mandatory requirements for each component in CFG_NDcPP-WIDS-WLANAS_V1.0. This includes requirements that all conformant products must claim and requirements in CPP_ND_V2.2E that are modified by a PP-Module (e.g., by forcing that a certain selection be made or that a certain optional requirement must be included). These requirements were validated as part of the Ruckus SmartZone evaluation activities referenced above.

Table 6: Mandatory and Base-PP Modified SFRs

Requirement Class	Requirement Component	Verified By
CPP_ND_V2.2E		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Ruckus SmartZone
	FAU_GEN.2: User Identity Association	Ruckus SmartZone
	FAU_STG_EXT.1: Protected Audit Event Storage	Ruckus SmartZone
FCS: Cryptographic Security	FCS_CKM.1: Cryptographic Key Generation	Ruckus SmartZone
	FCS_CKM.2: Cryptographic Key Establishment	Ruckus SmartZone
	FCS_CKM.4: Cryptographic Key Destruction	Ruckus SmartZone (Iterated as "FCS_CKM.4" for "(v)SZ/vSZ-D" and "FCS_CKM.4(1)" for "AP")
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Ruckus SmartZone
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	Ruckus SmartZone
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	Ruckus SmartZone
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	Ruckus SmartZone
	FCS_RBG_EXT.1: Random Bit Generation	Ruckus SmartZone
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Management	Ruckus SmartZone
	FIA_PMG_EXT.1: Password Management	Ruckus SmartZone
	FIA_UAU_EXT.2: Password-based Authentication Mechanism	Ruckus SmartZone
	FIA_UIA_EXT.1: User Identification and Authentication	Ruckus SmartZone
	FIA_UAU.7: Protected Authentication Feedback	Ruckus SmartZone

Requirement Class	Requirement Component	Verified By
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	Ruckus SmartZone
	FMT_MTD.1/CoreData: Management of TSF Data	Ruckus SmartZone
	FMT_SMF.1: Specification of Management Functions	Ruckus SmartZone
	FMT_SMR.2: Restrictions on Security Roles	Ruckus SmartZone
FPT: Protection of TSF	FPT_APW_EXT.1: Protection of Administrator Passwords	Ruckus SmartZone
	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared symmetric and private keys)	Ruckus SmartZone
	FPT_STM_EXT.1: Reliable Time Stamps	Ruckus SmartZone
	FPT_TUD_EXT.1: Trusted Update	Ruckus SmartZone
	FPT_TST_EXT.1: TSF Testing	Ruckus SmartZone
FTA: TOE Access	FTA_SSL_EXT.1: TSF-Initiated Session Locking	Ruckus SmartZone
	FTA_SSL.3: TSF-Initiated Termination	Ruckus SmartZone
	FTA_SSL.4: User-Initiated Termination	Ruckus SmartZone
	FTA_TAB.1: Default TOE Access Banners	Ruckus SmartZone
FTP: Trusted Path/Channels	FTP_ITC.1 Inter-TSF Trusted Channel	Ruckus SmartZone
	FTP_TRP.1/Admin: Trusted Path	Ruckus SmartZone
From MOD_WIDS_V1.0 – Modified SFRs when CPP_ND_V2.2E is the Base-PP		
FAU: Security Audit	FAU_GEN_EXT.1: Security Audit Data Generation for Distributed Components	Ruckus SmartZone
	FAU_STG_EXT.1: Protected Audit Event Storage	Ruckus SmartZone
FCO: Communication	FCO_CPC_EXT.1: Communication Partner Control	Ruckus SmartZone (titled "Component Registration Channel Definition" in ST)
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	Ruckus SmartZone
FTP: Trusted Paths/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Ruckus SmartZone
From MOD_WLANAS_V1.0 – Modified SFRs when CPP_ND_V2.2E is the Base-PP		
FAU: Security Audit	FAU_GEN_EXT.1: Security Audit Generation	Ruckus SmartZone
	FAU_STG_EXT.1: Protected Audit Event Storage	Ruckus SmartZone
	FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs	Ruckus SmartZone

Requirement Class	Requirement Component	Verified By
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	Ruckus SmartZone
FCS: Cryptographic Support	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Ruckus SmartZone
FPT: Protection of the TSF	FPT_TST_EXT.1: TSF Testing	Ruckus SmartZone
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Ruckus SmartZone

Table 7 contains the "base" requirements specific to the TOE.

Table 7: TOE SFRs

Requirement Class	Requirement Component	Verified By
From MOD_WIDS_V1.0		
FAU: Security Audit	FAU_ARP.1: Security Alarms	Ruckus SmartZone
	FAU_ARP_EXT.1: Security Alarm Filtering	Ruckus SmartZone
	FAU_GEN.1/WIDS: Audit Data Generation (WIDS)	Ruckus SmartZone
	FAU_IDS_EXT.1: Intrusion Detection System – Intrusion Detection Methods	Ruckus SmartZone
	FAU_INV_EXT.1: Environmental Inventory	Ruckus SmartZone
	FAU_INV_EXT.2: Characteristics of Environmental Objects	Ruckus SmartZone
	FAU_INV_EXT.3: Location of Environmental Objects	Ruckus SmartZone
	FAU_RPT_EXT.1: Intrusion Detection System – Reporting Methods	Ruckus SmartZone
	FAU_SAA.1: Potential Violation Analysis	Ruckus SmartZone
	FAU_WID_EXT.1: Wireless Intrusion Detection – Malicious Environmental Objects	Ruckus SmartZone
	FAU_WID_EXT.2: Wireless Intrusion Detection – Passive Information Flow Monitoring	Ruckus SmartZone
FDP: User Data Protection	FDP_IFC.1: Subset Information Flow Control	Ruckus SmartZone

Requirement Class	Requirement Component	Verified By
FMT: Security Management	FMT_SMF.1/WIDS: Specification of Management Functions (WIDS)	Ruckus SmartZone
From MOD_WLANAS_V1.0		
FAU: Security Audit	FAU_GEN.1.1/WLAN: Audit Data Generation	Ruckus SmartZone
FCS: Cryptographic Support	FCS_CKM.1/WPA: Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)	Ruckus SmartZone
	FCS_CKM.2/GTK: Cryptographic Key Distribution (GTK)	Ruckus SmartZone
	FCS_CKM.2/PMK: Cryptographic Key Distribution (PMK)	Ruckus SmartZone
FIA: Identification and Authentication	FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication	Ruckus SmartZone
	FIA_UAU.6: Re-Authenticating	Ruckus SmartZone
FMT: Security Management	FMT_SMF.1/AccessSystem: Specification of Management Functions (WLAN Access Systems)	Ruckus SmartZone
	FMT_SMR_EXT.1: No Administration from Client	Ruckus SmartZone
FPT: Protection of the TSF	FPT_FLS.1: Failure with Preservation of Secure State	Ruckus SmartZone
FTA: TOE Access	FTA_TSE.1: TOE Session Establishment	Ruckus SmartZone
FTP: Trusted Path/Channels	FTP_ITC.1/Client: Inter-TSF Trusted Channel (WLAN Client Communications)	Ruckus SmartZone

Table 8 contains the "**Optional**" (including Strictly Optional) requirements contained in Appendix A, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
CPP_ND_V2.2E		
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage	cPP Evaluation
	FAU_STG_EXT.2/LocSpace: Counting Lost Audit Data	cPP Evaluation
	FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss	cPP Evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	Ruckus SmartZone

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLSC_EXT.2: DTLS Client Support for Mutual Authentication	cPP Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Support for Mutual Authentication	cPP Evaluation
	FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication	cPP Evaluation
	FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication	cPP Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certification Validation	Ruckus SmartZone
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	Ruckus SmartZone
FTP: Trusted Path/Channels	FTP_TRP.1/Join: Trusted Path	Ruckus SmartZone
From MOD_WIDS_V1.0		
FAU: Security Audit	FAU_WID_EXT.3: Wireless Intrusion Detection – Non-Wireless Spectrum Monitoring	Module Evaluation
	FAU_WID_EXT.4: Wireless Intrusion Detection – Wireless Spectrum Analysis	Module Evaluation
From MOD_WLANAS_V1.0 (Strictly Optional)		
FCS: Cryptographic Support	FCS_CKM.2/DISTRIB: Cryptographic Key Distribution (802.11 Keys)	Module Evaluation

Table 9 contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
CPP_ND_V2.2E		
FAU: Security Audit	FAU_GEN_EXT.1: Security Audit Data Generation for Distributed TOE Component	Ruckus SmartZone (title "Security Audit Generation" in ST)
	FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs	Ruckus SmartZone
	FAU_STG_EXT.5: Protected Remote Audit Event Storage for Distributed TOEs	Ruckus SmartZone
	FCS_DTLSC_EXT.1: DTLS Client Protocol Without Mutual Authentication	cPP Evaluation

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_DTLSS_EXT.1: DTLS Server Protocol Without Mutual Authentication	cPP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	Ruckus SmartZone
	FCS_IPSEC_EXT.1: IPsec Protocol	Ruckus SmartZone
	FCS_NTP_EXT.1: NTP Protocol	Ruckus SmartZone
	FCS_SSHC_EXT.1: SSH Client Protocol	Ruckus SmartZone
	FCS_SSHS_EXT.1: SSH Server Protocol	Ruckus SmartZone
	FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication	Ruckus SmartZone
	FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication	Ruckus SmartZone
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Ruckus SmartZone
	FIA_X509_EXT.2: X.509 Certificate Authentication	Ruckus SmartZone
	FIA_X509_EXT.3: X.509 Certificate Requests	Ruckus SmartZone
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	cPP Evaluation
FMT: Security Management	FMT_MOF.1/Services: Management of Security Functions Behaviour	cPP Evaluation
	FMT_MOF.1/AutoUpdate: Management of Security Functions Behaviour	cPP Evaluation
	FMT_MOF.1/Functions: Management of Security Functions Behaviour	cPP Evaluation
	FMT_MTD.1/CryptoKeys: Management of TSF Data	Ruckus SmartZone
From MOD_WIDS_V1.0		
FAU: Security Audit	FAU_ANO_EXT.1: Anomaly-Based Intrusion Detection	Module Evaluation
	FAU_SIG_EXT.1: Signature-Based Intrusion Detection	Module Evaluation
	FAU_STG_EXT.1/PCAP: Protected Audit Event Storage (Packet Captures)	Module Evaluation
From MOD_WLANAS_V1.0		
FCS: Cryptographic Support	FCS_RADSEC_EXT.1: RadSec	Ruckus SmartZone
	FCS_RADSEC_EXT.2: RadSec using Pre-Shared Keys	Module Evaluation
	FCS_RADSEC_EXT.3: RadSec using Pre-Shared Keys and RSA	Module Evaluation

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Ruckus SmartZone

Table 10 contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the Identification section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant ACE workunits and has indicated its verification through "Module Evaluation."

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
CPP_ND_V2.2E		
No objective requirements defined in CPP_ND_V2.2E.		
From MOD_WIDS_V1.0		
FAU: Security Audit	FAU_INV_EXT.4: Detection of Unauthorized Connections	Module Evaluation
	FAU_INV_EXT.5: Signal Library	Module Evaluation
	FAU_MAC_EXT.1: Device Impersonation	Module Evaluation
	FAU_WIP_EXT.1: Wireless Intrusion Prevention	Module Evaluation
FPT: Protection of the TSF	FPT_FLS.1: Basic Internal TSF Data Transfer Protection	Module Evaluation
From MOD_WLANAS_V1.0		
No objective requirements defined in MOD_WLANAS_V1.0		

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by CPP_ND_V2.2E. The SARs defined in that PP are applicable to MOD_WIDS_V1.0 and MOD_WLANAS_V1.0, as well as CFG_NDcPP-WIDS-WLANAS_V1.0 as a whole.

7 Results of the Evaluation

Note that for APE and ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 11: Evaluation Results: CPP_ND_V2.2E

ACE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	PP Evaluation
APE_CCL.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation
APE_OBJ.1	Pass	PP Evaluation
APE_ECD.1	Pass	PP Evaluation
APE_REQ.1	Pass	PP Evaluation

Table 12: Evaluation Results: MOD_WIDS_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.1	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.1	Pass	Module evaluation

Table 13: Evaluation Results: MOD_WLANAS_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module evaluation
ACE_CCL.1	Pass	Module evaluation
ACE_SPD.1	Pass	Module evaluation
ACE_OBJ.1	Pass	Module evaluation
ACE_ECD.1	Pass	Module evaluation
ACE_REQ.1	Pass	Module evaluation

Table 14: Evaluation Results: CFG_NDcPP-WIDS-WLANAS_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_CCO.1	Pass	PP-Config evaluation
ACE_MCO.1	Pass	PP-Config evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_WIDS_V1.0 and MOD_WLANAS_V1.0 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020.

[7] PP-Module for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), Version 1.0, 2020-09-30.

[8] PP-Module for Wireless Local Area Network (WLAN) Access System, Version 1.0, 2022-03-31

[9] PP-Configuration for Network Devices, Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS), and Wireless Local Area Network (WLAN) Access Systems, Version 1.0, 05 April 2023

[10] Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3 Security Target, Version 0.6, 09/18/2023

[11] Assurance Activity Report for Ruckus SmartZone WLAN Controllers & Access Points with WIDS, R5.2.1.3, Version 0.4, 09/18/2023