National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for
Network Devices and MACsec Ethernet Encryption

Version 1.0

29 March 2023

Report Number: CCEVS-VR-PP-0093
Dated: 08 August 2024
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 Protection Profile (PP)-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0 (CFG_NDcPP-MACSEC_V1.0). This 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 and the PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACSEC_V1.0). It presents a summary of the CFG_NDcPP-MACSEC_V1.0 and the evaluation results.

Gossamer Security Solutions, located in Columbia, Maryland, performed the evaluation of the CFG_NDcPP-MACSEC_V1.0 and the CPP_ND_V2.2E Base-PP and MOD_MACSEC_V1.0, contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Aruba, a Hewlett Packard Enterprise Company 6300M and 8360v2 Switch Series MACsec (Aruba MACsec Switch).

This evaluation addressed the base security functional requirements (SFRs) of the CPP_ND_V2.2E Base-PP and MOD_MACSEC_V1.0 PP-Module. The Validation Report (VR) author independently performed an additional review of the PP-Configuration and Module as part of the completion of this VR, to confirm they met the claimed APE and ACE requirements.

The evaluation determined the CFG_NDcPP-MACSEC_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 Module identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from CPP_ND_V2.2E and MOD_MACSEC_V1.0; completion of the ASE workunits satisfied the APE workunits for CPP_ND_V2.2E and the ACE workunits for the PP-Module, but only for the materials defined in this PP-Module, and only when the PP-Module is 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-Module. 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-MACSEC_V1.0, CPP_ND_V2.2E, and MOD_MACSEC_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 the Aruba MACsec Switch, performed by Gossamer Security Solutions, Inc. in Columbia, Maryland.

This evaluation addressed the base SFRs of MOD_MACSEC_V1.0 as part of CFG_NDcPP-MACSEC_V1.0.

MOD_MACSEC_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains optional and selection-based 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.

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-Module. 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-MACSEC_V1.0 were evaluated.

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

PP-Configuration	PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 2023-03-29
Base-PP	collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020
Module in PP-Configuration	PP-Module for MACsec Ethernet Encryption, Version 1.0, 2023-03-02
ST (Base)	Aruba, a Hewlett Packard Enterprise company 6300M and 8360v2 Switch Series MACsec Security Target , Version 1.0, April 10, 2024
Assurance Activity Report (Base)	Assurance Activity Report for Aruba, a Hewlett Packard Enterprise company 6300M and 8360v2 Switch Series MACsec, Version 0.3, April 13, 2024
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-MACSEC_V1.0 Description

CFG_NDcPP-MACSEC_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 MACsec Ethernet Encryption, Version 1.0, (MOD_MACSEC_V1.0)

This PP-Configuration defines a baseline set of SFRs for MACsec Ethernet Encryption (defined in CPP_ND_V2.2E) that is bundled with agent applications to enforce configured policies on MACsec Systems (defined in MOD_MACSEC_V1.0).

MACsec devices allow authorized systems using Ethernet Transport to maintain confidentiality of transmitted data and to take measures against frames that are transmitted or modified by unauthorized devices.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_NDcPP-MACSEC_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

Assumption Name	Assumption Definition
	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.
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

Assumption Name	Assumption Definition
	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_MACSEC_V1.0	
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. This document does not define any additional assumptions.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_NDcPP-MACSEC_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.
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

Threat Name	Threat Definition
	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_MACSEC_V1.0	
T.DATA_INTEGRITY	An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient. Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization. A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.

Threat Name	Threat Definition
T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS	An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit. A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_NDcPP-MACSEC_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_MACSEC_V1.0	
No organizational security policies for the TOE defined in MOD_MACSEC_V1.0.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_NDcPP-MACSEC_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_MACSEC_V1.0	
O.AUTHENTICATION_MACSEC	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CAs) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity.
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that

TOE Security Objective	TOE Security Objective Definition
	experience excessive failures and by limiting access to security-relevant data that administrators do not need to view.
O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.PORT_FILTERING_MACSEC	To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs).
O.REPLAY_DETECTION	A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs.
O.SYSTEM_MONITORING_MACSEC	To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs).
O.TSF_INTEGRITY	To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure if any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state.

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

Environmental Security Objective	Environmental Security Objective Definition
	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 • 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_MACSEC_V1.0	
No security objectives for the operational environment defined in MOD_MACSEC_V1.0.	

5 Functional Requirements

As indicated above, CFG_NDcPP-MACSEC_V1.0 includes CPP_ND_V2.2E and MOD_MACSEC_V1.0.

Requirements in the MOD_MACSEC_V1.0 are comprised of modified Base-PP, "base", and additional requirements that are optional or selection-based.

Table 6 defines the mandatory requirements for each component in CFG_NDcPP-MACSEC_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 Aruba MACsec Switch 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	Aruba MACsec Switch
	FAU_GEN.2: User Identity Association	Aruba MACsec Switch
	FAU_STG_EXT.1: Protected Audit Event Storage	Aruba MACsec Switch
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Aruba MACsec Switch
	FCS_CKM.2: Cryptographic Key Establishment	Aruba MACsec Switch
	FCS_CKM.4: Cryptographic Key Destruction	Aruba MACsec Switch
	FCS_COP.1/DataEncryption: Cryptographic Operation (AES Data Encryption/Decryption)	Aruba MACsec Switch
	FCS_COP.1/Hash: Cryptographic Operation (Hash Algorithm)	Aruba MACsec Switch
	FCS_COP.1/KeyedHash: Cryptographic Operation (Keyed Hash Algorithm)	Aruba MACsec Switch
	FCS_COP.1/SigGen: Cryptographic Operation (Signature Generation and Verification)	Aruba MACsec Switch
	FCS_RBG_EXT.1: Random Bit Generation	Aruba MACsec Switch
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Management	Aruba MACsec Switch
	FIA_PMG_EXT.1: Password Management	Aruba MACsec Switch
	FIA_UIA_EXT.1: User Identification and Authentication	Aruba MACsec Switch
	FIA_UAU_EXT.2: Password-based Authentication Mechanism	Aruba MACsec Switch
	FIA_UAU.7: Protected Authentication Feedback	Aruba MACsec Switch
FMT: Security Management	FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	Aruba MACsec Switch

Requirement Class	Requirement Component	Verified By
	FMT_MTD.1/CoreData: Management of TSF Data	Aruba MACsec Switch
	FMT_SMF.1: Specification of Management Functions	Aruba MACsec Switch
	FMT_SMR.2: Restrictions on Security Roles	Aruba MACsec Switch
FPT: Protection of TSF	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all pre-shared symmetric and private keys)	Aruba MACsec Switch
	FPT_APW_EXT.1: Protection of Administrator Passwords	Aruba MACsec Switch
	FPT_TST_EXT.1: TSF Testing	Aruba MACsec Switch
	FPT_TUD_EXT.1: Trusted Update	Aruba MACsec Switch
	FPT_STM_EXT.1: Reliable Time Stamps	Aruba MACsec Switch
FTA: TOE Access	FTA_SSL_EXT.1: TSF-Initiated Session Locking	Aruba MACsec Switch
	FTA_SSL.3: TSF-Initiated Termination	Aruba MACsec Switch
	FTA_SSL.4: User-Initiated Termination	Aruba MACsec Switch
	FTA_TAB.1: Default TOE Access Banners	Aruba MACsec Switch
FTP: Trusted Path/Channels	FTP_ITC.1 Inter-TSF Trusted Channel	Aruba MACsec Switch
	FTP_TRP.1/Admin: Trusted Path	Aruba MACsec Switch
From MOD_MACSEC_V1.0 – Modified SFRs when CPP_ND_V2.2E is the Base-PP		
No modified Base-PP SFRs defined in MOD_MACSEC_V1.0.		

Table 7 contains the "base" requirements from the PP-Module that all TOEs conforming to this PP-Configuration must claim.

Table 7: PP-Module Mandatory SFRs

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_GEN.1.1/MACSEC: Audit Data Generation (MACsec)	Aruba MACsec Switch
FCS: Cryptographic Support	FCS_COP.1/CMAC: Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	Aruba MACsec Switch
	FCS_COP.1/MACSEC: Cryptographic Operation (MACsec AES Data Encryption and Decryption)	Aruba MACsec Switch
	FCS_MACSEC_EXT.1: MACsec	Aruba MACsec Switch
	FCS_MACSEC_EXT.2: MACsec Integrity and Confidentiality	Aruba MACsec Switch
	FCS_MACSEC_EXT.3: MACsec Randomness	Aruba MACsec Switch

Requirement Class	Requirement Component	Verified By
	FCS_MACSEC_EXT.4: MACsec Key Usage	Aruba MACsec Switch
	FCS_MKA_EXT.1: MACsec Key Agreement	Aruba MACsec Switch
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Aruba MACsec Switch
FMT: Security Management	FMT_SMF.1/MACSEC: Specification of Management Functions (MACsec)	Aruba MACsec Switch
FPT: Protection of the TSF	FPT_CAK_EXT.1: Protection of CAK Data	Aruba MACsec Switch
	FPT_FLS.1: Failure with Preservation of Secure State	Aruba MACsec Switch
	FPT_RPL.1: Replay Detection	Aruba MACsec Switch
FTP: Trusted Path/Channels	FTP_ITC.1/MACSEC: Inter-TSF Trusted Channel (MACsec Communications)	Aruba MACsec Switch

Tables 8, 9, and 10 contain the "**Optional,**" **"Objective,"** and "**Implementation-Based**" requirements contained in Appendix A of the Base-PP and PP-Module, 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	PP Evaluation
	FAU_STG_EXT.2/LocSpace: Counting Lost Audit Data	PP Evaluation
	FAU_STG_EXT.3/LocSpace: Action in Case of Possible Audit Data Loss	PP Evaluation
FCO: Communication	FCO_CPC_EXT.1: Component Registration Channel Definition	PP Evaluation
FCS: Cryptographic Support	FCS_DTLSC_EXT.2: DTLS Client Support for Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.2: DTLS Server Support for Mutual Authentication	PP Evaluation
	FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication	Aruba MACsec Switch
	FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication	PP Evaluation

Requirement Class	Requirement Component	Verified By
FIA: Identification and Authentication	FIA_X509_EXT.1/ITT: X.509 Certification Validation	PP Evaluation
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	PP Evaluation
FTP: Trusted Path/Channels	FTP_TRP.1/Join: Trusted Path	PP Evaluation
From MOD_MACSEC_V1.0		
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Attempt Limiting	Module Evaluation
FPT: Protection of the TSF	FPT_DDP_EXT.1: Data Delay Protection	Module Evaluation
	FPT_RPL_EXT.1: Replay Protection for XPN	Aruba MACsec Switch
FTP: Trusted Path/Channels	FTP_TRP.1/MACSEC: Trusted Path (MACsec Administration)	Module Evaluation

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
From CPP_ND_V2.2E		
No objective SFRs defined in CPP_ND_V2.2E.		
From MOD_MACSEC_V1.0		
No objective SFRs defined in MOD_MACSEC_V1.0.		

Table 10: Implementation-Based Requirements

Requirement Class	Requirement Component	Verified By
From CPP_ND_V2.2E		
No implementation-based SFRs defined in CPP_ND_V2.2E.		
From MOD_MACSEC_V1.0		
No implementation-based SFRs defined in MOD_MACSEC_V1.0.		

Table 11 contains the "**Selection-Based**" requirements contained in Appendix B of the Base-PP and PP-Module, 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 11: 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	PP Evaluation
	FAU_STG_EXT.4: Protected Local Audit Event Storage for Distributed TOEs	PP Evaluation
	FAU_STG_EXT.5: Protected Remote Audit Event Storage for Distributed TOEs	PP Evaluation
FCS: Cryptographic Support	FCS_DTLSC_EXT.1: DTLS Client Protocol Without Mutual Authentication	PP Evaluation
	FCS_DTLSS_EXT.1: DTLS Server Protocol Without Mutual Authentication	PP Evaluation
	FCS_HTTPS_EXT.1: HTTPS Protocol	Aruba MACsec Switch
	FCS_IPSEC_EXT.1: IPsec Protocol	PP Evaluation
	FCS_NTP_EXT.1: NTP Protocol	PP Evaluation
	FCS_SSHC_EXT.1: SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	Aruba MACsec Switch
	FCS_TLSC_EXT.1: TLS Client Protocol Without Mutual Authentication	Aruba MACsec Switch
	FCS_TLSS_EXT.1: TLS Server Protocol Without Mutual Authentication	Aruba MACsec Switch
FIA: Identification and Authentication	FIA_X509_EXT.1/Rev: X.509 Certificate Validation	Aruba MACsec Switch
	FIA_X509_EXT.2: X.509 Certificate Authentication	Aruba MACsec Switch
	FIA_X509_EXT.3: X.509 Certificate Requests	Aruba MACsec Switch
FPT: Protection of the TSF	FPT_TUD_EXT.2: Trusted Update Based on Certificates	PP Evaluation
FMT: Security Management	FMT_MOF.1/Services: Management of Security Functions Behaviour	PP Evaluation
	FMT_MOF.1/AutoUpdate: Management of Security Functions Behaviour	PP Evaluation
	FMT_MOF.1/Functions: Management of Security Functions Behaviour	PP Evaluation
	FMT_MTD.1/CryptoKeys: Management of TSF Data	Aruba MACsec Switch

Requirement Class	Requirement Component	Verified By
From MOD_MACSEC_V1.0		
FCS: Cryptographic Support	FCS_DEVID_EXT.1: Secure Device Identifiers	Module Evaluation
	FCS_EAPTLS_EXT.1: EAP-TLS Protocol	Module Evaluation
	FCS_SNMP_EXT.1: SNMP Protocol	Module Evaluation
FMT: Security Management	FMT_SNMP_EXT.1: SNMP Management	Module Evaluation

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_MACSEC_V1.0, as well as CFG_NDcPP-MACSEC_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 12: 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 13: Evaluation Results: MOD_MACSEC_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-MACSEC_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_MACSEC_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 MACsec Ethernet Encryption, Version 1.0, 2023-03-02.

[8] PP-Configuration for Network Devices and MACsec Ethernet Encryption, Version 1.0, 2023-03-29.

[9] Aruba, a Hewlett Packard Enterprise company 6300M and 8360v2 Switch Series MACsec Security Target , Version 1.0, April 10, 2024.

[10] Assurance Activity Report for Aruba, a Hewlett Packard Enterprise company 6300M and 8360v2 Switch Series MACsec, Version 0.3, April 13, 2024.