National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Aruba, a Hewlett Packard Enterprise Company Aruba Mobility Controller with ArubaOS 8.6

Report Number: CCEVS-VR-11110-2021
Dated: 02/05/2021
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

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
Linda Morrison
Lisa Mitchell
Jenn Dotson
Clare Olin
The MITRE Corporation

Common Criteria Testing Laboratory

Khai Van
Katie Sykes
Andrew Ding
Gossamer Security Solutions, Inc.
Catonsville, 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 Aruba Mobility Controller Series with ArubaOS 8.6 solution provided by Aruba, a Hewlett Packard Enterprise Company. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Catonsville, MD, United States of America, and was completed in February 2021. The information in this report is largely derived from the proprietary Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions and summarized in the publicly available Assurance Activity Report (AAR) for this evaluation. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 2020-03-06 which includes the following components:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 (STFFW13)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (VPNGW10)

The Target of Evaluation (TOE) is Aruba Mobility Controller with ArubaOS 8.6. The TOE is a multi-purpose network device with stateful traffic filter firewall and VPN gateway capabilities.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are

correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Aruba Mobility Controller with ArubaOS 8.6 (NDcPP21/STFFW13/VPNGW10) Security Target, Version 1.0, 02/05/2021 and analysis performed by the validation team.

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 Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Aruba Mobility Controller with ArubaOS 8.6 (Specific models identified in Section 3.1)
Protection Profile	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 2020-03-06 which includes the following components: • collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21) • PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 (STFFW13) • PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (VPNGW10)
ST	Aruba Mobility Controller with ArubaOS 8.6 (NDcPP21/STFFW13/VPNGW10) Security Target, Version 1.0, 02/05/2021
Evaluation Technical Report	Aruba Mobility Controller with ArubaOS 8.6, Version 0.4, 02/05/2021

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 Extended, CC Part 3 conformant
Sponsor	Aruba, a Hewlett Packard Enterprise Company
Developer	Aruba, a Hewlett Packard Enterprise Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Sheldon Durrant, Linda Morrison, Lisa Mitchell, Jenn Dotson, Clare Olin The MITRE Corporation

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

Aruba Mobility Controllers (MCs) are hardware appliances consisting of a multicore network processor, Ethernet interfaces, and required supporting circuitry and power supplies enclosed in a metal chassis. Aruba Virtual Mobility Controllers (VMCs) consist of a 64-bit virtualized software-based managed platform on virtual machine (VM) architecture. The Aruba VMC operates on x86 platforms in a hypervisor environment.

The ArubaOS software running on the MCs and VMCs consists of two main components:

- Control Plane (CP) – implements functions which can be handled at lower speeds such as Mobility Controller system management (CLI and Web GUI), VMC system management (CLI and Web GUI), user authentication (e.g. RADIUS), Internet Key Exchange (IKE), auditing/logging (syslog), Wireless IDS (WIDS), and termination of protocols operating at the system level (e.g. SSH, TLS, NTP, etc.). The Control Plane runs the Linux operating system along with various user-space applications (described below).
- Data Plane (DP) - implements functions that must be handled at high speeds such as high-speed switching functions (forwarding, VLAN tagging/enforcement, bridging), termination of 802.11 associations/sessions, tunnel termination (IPsec), stateful firewall and deep packet inspection functions, and cryptographic acceleration. The Data Plane runs a lightweight, proprietary real-time OS which is known as "SOS" (an acronym which used to mean "SiByte Operating System" for an earlier generation of Mobility Controller that used the SiByte CPU). On the Mobility Controller hardware appliances, SOS runs on separate CPU cores. On the Virtual Mobility Controller appliances, SOS is a process running under Linux.

The Control Plane and Data Plane are inseparable. Administrators install the MC software by loading a single file, identified as "ArubaOS". Administrators install the VMC by creating a virtual machine in the ESXi client interface and then applying the VMC OVF template to the virtual machine, identified as "ArubaOS". Internally, the controllers unpack the ArubaOS software image into its various components. A given ArubaOS software image has a single version number and includes all software components necessary to operate the MC and VMC appliances as well as the APs which are in the operating environment of the TOE.

The CP runs the Linux OS, along with various custom user-space applications which provide the following CP functions:

- Monitors and manages critical system resources, including processes, memory, and flash
- Manages system configuration and licensing

- Manages an internal database used to store licenses, user authentication information, etc
- Provides network anomaly detection, hardware monitoring, mobility management, wireless management, and radio frequency management services
- Provides a Command Line Interface (CLI)
- Provides a web-based (HTTPS/TLS) management UI for the MCs and VMCs
- Provides authentication services for the system management interfaces (CLI, web GUI)
- Provides IPsec key management services for VPN users, and connections with other Aruba mobility controllers
- Provides network time protocol service, point to point tunneling protocol services for users, layer 2 tunneling protocol services for users, SSH services for incoming management connections, SNMP client/agent services, and protocol independent multicast (routing) services for the controller
- Provides syslog services by sending logs to the operating environment

The Linux OS running on the CP is a version 2.6.32 kernel for the MCs and a version 3.18.26 kernel for the VMCs. Linux is a soft real-time, multi-threaded operating system that supports memory protection between processes. Only Aruba provided interfaces are used, and the CLI is a restricted command set. Administrators do not have access to the Linux command shell or operating system.

All Aruba Mobility Controller and Virtual Mobility Controller models run the same ArubaOS 8.6 software and include the same ArubaOS Crypto Module. Regardless of the different hardware and virtual platforms, the security functionality remains the same. The differences in the platforms are in the processing speed, throughput, memory capacity, storage, physical interfaces, number of ports, etc., and are based on performance and scalability requirements. All models run the same code with the only differences being the hardware specific code for the differently scaled hardware and the virtual nature of the hardware ports on the VMs.

The Virtual Mobility Controller uses gigabit Ethernet interfaces just as a hardware-based mobility controller does, but these interfaces map to virtual interfaces created in the underlying hypervisor. Those interfaces, in turn, may map directly to physical ports. The device drivers on all VM platforms are identical because the ArubaOS is being run on a hypervisor. Within the hypervisor, there may be slight differences in device drivers (mostly for network interfaces), however, the device drivers are not used to enforce any TOE security functions.

4 Security Policy

The TOE provides the security functionality required by NDcPP21, STFFW13, and VPNGW10 as listed below:

4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events including start-up and shutdown of the TOE, all administrator actions, and all Protection Profile required auditable events. The TOE can be configured to store the logs locally or alternately configured to send the logs to a designated syslog server in the operational environment.

4.2 Cryptographic support

The TOE includes cryptographic modules that provide key management, random bit generation, encryption/decryption, digital signature, and secure hashing and key-hashing features in support of higher level cryptographic protocols including IPsec, SSH, and TLS/HTTPS.

4.3 User Data Protection

The TOE ensures that any data packets passing through the TOE do not inadvertently contain any residual information that might be disclosed inappropriately.

4.4 Firewall

The TOE performs stateful packet filtering. Filtering rules may be applied to appliance Ethernet interfaces or to user-roles (wireless clients connecting through APs are placed into user-roles). Stateful packet filter policies are applied to user-roles to allow fine grained control over wireless traffic.

4.5 Identification and authentication

The TOE requires administrators to be identified and authenticated before they can access any TOE security functions. The TOE supports role-based authentication, so user accounts are assigned predefined roles which restrict them based on their assigned role. The TOE maintains these administrator and user attributes which can be defined locally with user names and passwords or can be defined in the context of RADIUS or TACACS+ services. Authentication can be either locally or remotely through an external authentication server, or internally. After an administrator-specified number of failed attempts, the user account is locked out. The TOE's password mechanism provides configuration for a minimum password length. The TOE also protects, stores and allows authorized administrators to load X.509.v3 certificates for use to support authentication for IPsec connections.

4.6 Security management

The TOE provides the administrator role the capability to configure and manage all TOE security functions including cryptographic operations, user accounts, passwords, advisory banner, session inactivity and TOE updates. The management functions are restricted to the administrator role. The role must have the appropriate access privileges or access will be denied. The TOE's cryptographic functions ensure that only secure values are accepted for security attributes.

4.7 Packet Filtering

The TOE may be used as a VPN gateway – a device at the edge of a private network that terminates an IPsec tunnel, which provides device authentication, confidentiality, and integrity of information traversing a public or untrusted network. The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. An administrator can configure security policies that determine whether to block, allow, or log a session based on traffic attributes such as the source and destination security zone, the source and destination IP address, the application, user, and the service.

4.8 Protection of the TSF

The TOE has an internal hardware clock that provides reliable time stamps used for auditing. The internal clock may be synchronized with a time signal obtained from an external trusted NTP server. The TOE stores passwords on flash using a SHA1 hash and does not provide any interfaces that allow passwords or keys to be read.

The TOE runs self-tests during power up and periodically during operation to ensure the correct operation of the cryptographic functions and TSF hardware. There is an option for the administrator to verify the integrity of stored TSF executable code.

The TOE includes mechanisms so that the administrator can determine the TOE version and update the TOE securely using digital signatures.

4.9 TOE Access

The TOE allows administrators to configure a session inactivity time limit for both administrator and wireless user sessions. When the configured time period of no activity has elapsed, the session is terminated. All users can also terminate their own sessions at any time. A warning banner is displayed at the management interfaces (Web GUI and CLI) to advise users on appropriate use and penalty for misuse of system.

In order to limit access to the administrative functions, the TOE can be configured to deny wireless clients and remote VPN clients based on the time/date, IP address (location), as well as information retained in a blacklist. The TOE assigns a private IP address (internal to the trusted network for which the TOE is the headend) to a VPN client upon successful establishment of a session.

4.10 Trusted path/channels

The TOE uses IPsec to provide an encrypted channel between itself and third-party trusted IT entities in the operating environment including Aruba access point(s), external syslog server, external authentication server, 802.1x authentication server, NTP server and VPN Gateway/Client. The TOE also uses IPsec to encrypt communications between TOE components.

The TOE secures remote communication with administrators by implementing TLS/HTTPS for remote Web UI access and SSHv2 for CLI access. In each case, both the integrity and disclosure protection is ensured via the secure protocol. If the negotiation of a secure session fails or if the user cannot be authenticated for remote administration, the attempted session will not be established.

5 Assumptions, Threats, and Clarification of Scope

The Security Problem Definition, including the assumptions and threats, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (NDcPP21)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 (STFFW13)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (VPNGW10)

That information has not been reproduced here and those particular Protection Profiles and PP-Modules (NDcPP21/STFFW13/VPNGW10) should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21/STFFW13/VPNGW10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that could benefit from clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the NDcPP21/STFFW13/VPNGW10 and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions either released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP21/STFFW13/VPNGW10 and the applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Aruba OS 8.6 Supplemental Guidance (Common Criteria Configuration Guidance), Version 1.10, February 05, 2021

To use the product in the evaluated configuration, the product must be configured as specified in that guide. Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device in its evaluated configuration. Consumers are encouraged to download the CC configuration guide from the NIAP website.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP21/STFFW13/VPNGW10) for Aruba Mobility Controller with ArubaOS 8.6, Version 1.0, 02/05/2021 (AAR). The AAR shows the test configuration, identifies the tested platforms and lists the test tools used in the evaluation.

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor provided Common Criteria Configuration Guidance document and performed the test activities specified in the NDcPP21/STFFW13/VPNGW10 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the Aruba Mobility Controller with ArubaOS version 8.6 with the following required software licenses installed:

- Policy Enforcement Firewall
- RFprotect
- Advanced Cryptography

The TOE includes the following hardware and virtual appliance models:

Mobility Controller Hardware Appliances

Product Model	Part Number(s)	CPU
Aruba 9004 Mobility Controller	R1B25A	Intel Atom C3508 (Denverton)
Aruba 7005 Mobility Controller	JW636A	Broadcom XLP208 (MIPS64)
Aruba 7008 Mobility Controller	JX932A	Broadcom XLP208 (MIPS64)
Aruba 7010 Mobility Controller	JW703A	Broadcom XLP208 (MIPS64)
Aruba 7024 Mobility Controller	JW707A	Broadcom XLP208 (MIPS64)
Aruba 7030 Mobility Controller	JW711A	Broadcom XLP208 (MIPS64)
Aruba 7205 Mobility Controller	JW740A	Broadcom XLP316 (MIPS64)
Aruba 7210 Mobility Controller	JW746A	Broadcom XLP416 (MIPS64)
Aruba 7220 Mobility Controller	JW754A	Broadcom XLP432 (MIPS64)
Aruba 7240 Mobility Controller	JW762A	Broadcom XLP432 (MIPS64)
Aruba 7240XM Mobility Controller	JW830A	Broadcom XLP432 (MIPS64)
Aruba 7280 Mobility Controller	JX914A	Broadcom XLP780 (MIPS64)

Mobility Controller Virtual Appliances

- MC-VA-50
- MC-VA-250
- MC-VA-1k

VM Platforms

The Mobility Controller Virtual Appliances are deployed on ESXi version 6.5.0. The following virtual machine platforms are included in the evaluated configuration:

Name	CPU	Memory
HPE EdgeLine EL8000	Intel Xeon Gold 6212U (Cascade Lake)	128GB
Klas Telecom VoyagerVM3	Intel Xeon D (Coffee Lake)	96GB
IAS VPN Gateway Module Classic Plus	Intel Core i7 (Skylake)	32GB
Pacstar 451/3	Intel Xeon D (Coffee Lake)	32GB
Pacstar 451/3	Intel Xeon E3 (Coffee Lake)	32GB
DTECH M3-SE-SVR4	Intel Xeon E3 v5-1505L (Skylake)	32GB
DTECH M3x	Intel Core i5 (Skylake)	32GB
GTS NXGEN-L11/12	Intel Core i7 (Coffee Lake)	16GB

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR as characterized in the publicly available Assurance Activity Report for this evaluation. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Aruba Mobility Controller with ArubaOS version 8.6 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21/STFFW13/VPNGW10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Aruba Mobility Controller with ArubaOS version 8.6 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP21/STFFW13/VPNGW10 related to the examination of the information contained in the TSS.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how

to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP21/STFFW13/VPNGW10 and recorded the results in a Test Report, summarized in the AAR.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. None of the public search for vulnerabilities or the fuzz testing uncovered any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- Exploit / Vulnerability Search Engine (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)

- Offensive Security Exploit Database (https://www.exploit-db.com/)

The search was performed on 01/16/2021 with the following search terms: aruba tcp", "aruba mobility controller", "arubaos", "aruba ipsec", "aruba ssh", "aruba tls", "arubaos openssl", "arubaos uboot", "aruba vmc", "aruba vpn", "esxi", “sos”, “sibyte”, “linux OS v2.6.32 kernel”, “linux OSv3.18.26 kernel”.

The validators reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFRs within the Security Target was evaluated. All other functionality provided by the devices, to include software or hardware that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Other functionality provided by devices in the operational environment, such as the audit server or authentication server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

For the TOE to be operated in the Common Criteria Mode the following software licenses must be installed on the device:

- Policy Enforcement Firewall
- RFprotect
- Advanced Cryptography

Note that authentication testing was not performed using TACACs, nor was testing performed on each individual VM platform included in the evaluated configuration; rather, equivalencies were claimed for those devices utilizing the VM and evaluated software.

The TOE's SSH server has a hardcoded function to shut down any invalid SSH session establishment after 2 tries. This function does not affect the TOE's ability to keep track of the number of authentication tries.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: Aruba Mobility Controller with ArubaOS 8.6 Security Target (NDcPP21/STFFW13/VPNGW10), Version 1.0, 02/05/2021.

13 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 in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **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 carried out by the CCEVS Validation Body leading to the issue 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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, September 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2017.

[4] Aruba Mobility Controller with ArubaOS 8.6 Security Target (NDcPP21/STFFW13/VPNGW10), Version 1.0, 02/05/2021

[5] Assurance Activity Report (NDcPP21/STFFW13/VPNGW10) for Aruba Mobility Controller with ArubaOS 8.6, Version 1.0, 02/05/2021 (AAR).

[6] Aruba OS 8.6 Supplemental Guidance (Common Criteria Configuration Guidance), Version 1.10, February 2021 (Admin Guide)