National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Aruba, a Hewlett Packard Enterprise Company

8000 Foothills Blvd

Roseville, CA 95747 USA

Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 (NDcPP20E)

Report Number: **CCEVS-VR-10872-2018**
Dated: **June 1, 2018**
Version: **0.4**

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Michelle Brown
NIAP

Meredith Hennan
Kenneth Stutterheim
The Aerospace Corporation
Columbia, MD

Common Criteria Testing Laboratory

Tammy Compton
Khai Van
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, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 solution provided by 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 May 2018. 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 collaborative Protection Profile for Network Devices, Version 2.0 + errata 20180314, 14 March 2018.

The Target of Evaluation (TOE) is the Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). 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, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 (NDcPP20E) Security Target, Version 0.6, May 31, 2018 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	HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series (Specific models identified in Section 3.1)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + errata 20180314, 14 March 2018
ST	HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series Security Target, Version 0.6, May 31, 2018
Evaluation Technical Report	Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04, version 0.4, May 31, 2018
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Hewlett Packard Enterprise Company
Developer	Hewlett Packard Enterprise Company
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.

Item	Identifier
CCEVS Validators	Meredith Hennan, Kenneth Stutterheim

3 Architectural Information

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

The Target of Evaluation (TOE) is Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04.

The TOE offers Layer 2 and Layer 3 feature sets including RIP, BGP, PoE+, and IPv4 and IPv6 functionalities. The Aruba 2930F, 2930M, 3810M, and 5400R Switch Series provide security, scalability, and ease of use for enterprise edge deployments.

The TOE is a family of switches designed to support scalability, security and high performance for campus networks.

3.1 TOE Evaluated Platforms

The evaluated configuration consists of the following models:

Series	Hardware Models	Processor
Aruba 2930F Switch Series	2930F 24G 4SFP+ Switch (JL253A) 2930F 48G 4SFP+ Switch (JL254A) 2930F 8G PoE+ 2SFP+ Switch (JL258A) 2930F 24G PoE+ 4SFP+ Switch (JL263A) 2930F 48G PoE+ 4SFP+ Switch (JL264A)	Dual Core ARM Coretex
Aruba 2930M Switch Series	2930M 24G 1-slot Switch (JL319A) 2930M 24G PoE+ 1-slot Switch (JL320A) 2930M 48G 1-slot Switch (JL321A) 2930M 48G PoE+ 1-slot Switch (JL322A) 2930M 40 Port 1G + 8 Port SmartRate PoE+ (JL323A) 2930M 24 Port SmartRate PoE+ (JL324A)	Dual Core ARM Coretex
Aruba 3810M Switch Series	3810M 24G 1-slot Switch (JL071A) 3810M 48G 1-slot Switch (JL072A) 3810M 24G PoE+ 1-slot Switch (JL073A) 3810M 48G PoE+ 1-slot Switch (JL074A) 3810M 16SFP+ 2-slot Switch (JL075A) 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch (JL076A)	Freescale P2020 Dual Core
Aruba 5400R Switch Series	5406R zl2 Switch (J9821A) 5412R zl2 Switch (J9822A) 5406R/5412R-24-port 10/100/1000Base-T PoE+ MACsec (No PSU) v3 zl2 Card (J9986A) 5406R/5412R-24p 1000BASE-T (No PSU) v3 zl2 Card (J9987A) 5406R/5412R-24p SFP (No PSU) v3 zl2 Card (J9988A) 5406R/5412R-12p PoE+ / 12p 1GbE SFP (No PSU) v3 zl2 Card (J9989A) 5406R/5412R-20p PoE+ / 4p SFP+ (No PSU) v3 zl2 Card (J9990A)	Freescale P2020 Dual Core

Series	Hardware Models	Processor
	5406R/5412R-20p PoE+ / 4p 1/25/5/XGT PoE+ (No PSU) v3 zl2 Card (J9991A) 5406R/5412R-20p PoE+ / 1p 40GbE QSPF+ (No PSU) v3 zl2 Card (J9992A) 5406R/5412R-8p 1G/10GbE SFP+ v3 (No PSU) v3 zl2 Card (J9993A) 5406R/5412R-2-port 40GbE QSFP+ (No PSU) v3 zl2 Card (J9996A)	

3.2 TOE Architecture

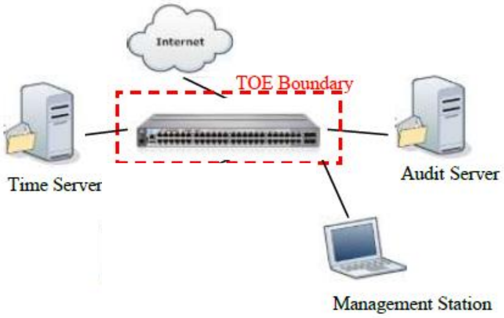
The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor and software that implements switching functions, configuration information and drivers. While hardware varies between different appliance models, the software code is shared across all platforms. It is in the software code that all the security functions claimed in this security target are enforced.

3.3 Physical Boundaries

Each TOE appliance runs a version of the Aruba software and has physical network connections to its environment to facilitate the switching of network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TOE may be accessed and managed through a PC or terminal in the environment which can be remote from or directly connected to the TOE.

The TOE can be configured to forward its audit records to an external SYSLOG server in the network environment. The TOE can also sync its time with an NTP server. The figure below shows the TOE depicted in its intended environment.



4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication

4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE is able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator and also to send the logs to a designated log server using TLS to protect the logs while in transit on the network.

4.2 Cryptographic support

The TOE provides CAVP certified cryptography in support of its SSHv2 and TLS protocol implementations. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature and secure hashing.

4.3 Identification and authentication

The TOE requires users to be identified and authenticated before they can use functions mediated by the TOE, with the exceptions of reading the login banner and passing network traffic in accordance with its configured switching rules. It provides the ability to assign attributes (user names, passwords and roles) and to authenticate users against these attributes. The TOE also provides X.509 certificate checking for its TLS connections.

4.4 Security management

The TOE provides Command Line Interface (CLI) commands and a web GUI to access the security management functions necessary to manage its security policies. All administrative activity and functions including security management commands are limited to authorized users (i.e., administrators) only after they have provided acceptable user identification and authentication data to the TOE. The security management functions are controlled through the use of roles that can be assigned to TOE users. The TOE supports the following roles: Manager and Operator. The Manager role can make changes to the TOE configuration while the Operator role is a read-only role.

4.5 Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects stored passwords and cryptographic keys so they are not directly accessible in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment. The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operation environment. The TOE performs self-tests to detect failure and protect itself from malicious updates.

4.6 TOE access

The TOE can be configured to display a logon banner before a user session is established. The TOE enforces inactivity timeouts for local and remote sessions.

4.7 Trusted path/channels

The TOE protects interactive communication with administrators using SSH for CLI and TLS for the web GUI to ensure both integrity and disclosure protection. If the negotiation of an encrypted session fails or if the user does not have authorization for remote administration, then the connection will not be established.

The TOE protects communication with network peers such as a log server, using TLS connections to prevent unintended disclosure or modification of logs.

5 Assumptions

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

- collaborative Protection Profile for Network Devices, Version 2.0 + errata 20180314, 14 March 2018

That information has not been reproduced here and the NDcPP20E 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 NDcPP20E 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.

6 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need 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 collaborative Protection Profile for Network Devices 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 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 NDcPP20E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7 Documentation

The following documents were available with the TOE for evaluation:

- Common Criteria Configuration Guidance Network Device Collaboration Protection Profile, Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series, Version 1.4, May 22, 2018

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.

8 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 (NDcPP20E) for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04, version 0.4, May 31, 2018 (AAR). The AAR shows the test configuration, provides the tested platforms and lists the test tools.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

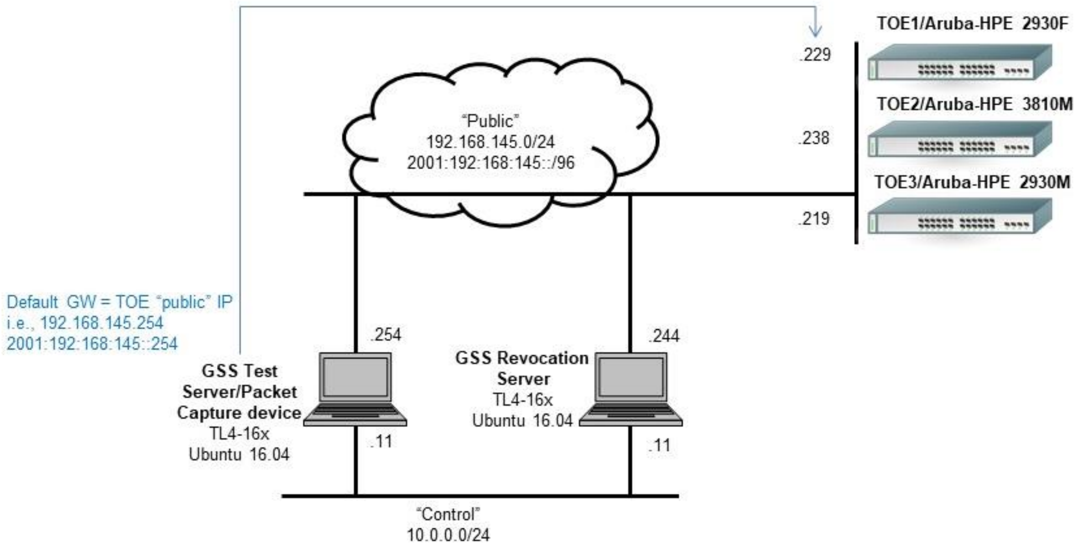
The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP20E including the tests associated with optional requirements.

8.3 Test Software

- SSH Client – Putty version 6.6.1p1
- Big Packet Putty version 6.2
- Wireshark version 2.4.4
- Tcpdump version 4.9.2
- Libpcap version 1.7.4-2

- Stunnel version 5.30-1
- ntp server version 4.2.8
- rsyslog version 8.16
- freeradius version 3.0.15

8.4 Test Environment



9 Evaluated Configuration

The evaluated configuration consists of the following series and models

Series	Hardware Models	Processor
Aruba 2930F Switch Series	2930F 24G 4SFP+ Switch (JL253A) 2930F 48G 4SFP+ Switch (JL254A) 2930F 8G PoE+ 2SFP+ Switch (JL258A) 2930F 24G PoE+ 4SFP+ Switch (JL263A) 2930F 48G PoE+ 4SFP+ Switch (JL264A)	Dual Core ARM Coretex
Aruba 2930M Switch Series	2930M 24G 1-slot Switch (JL319A) 2930M 24G PoE+ 1-slot Switch (JL320A) 2930M 48G 1-slot Switch (JL321A) 2930M 48G PoE+ 1-slot Switch (JL322A) 2930M 40 Port 1G + 8 Port SmartRate PoE+ (JL323A) 2930M 24 Port SmartRate PoE+ (JL324A)	Dual Core ARM Coretex
Aruba 3810M Switch Series	3810M 24G 1-slot Switch (JL071A) 3810M 48G 1-slot Switch (JL072A) 3810M 24G PoE+ 1-slot Switch (JL073A) 3810M 48G PoE+ 1-slot Switch (JL074A) 3810M 16SFP+ 2-slot Switch (JL075A) 3810M 40G 8 HPE Smart Rate PoE+ 1-slot Switch (JL076A)	Freescale P2020 Dual Core

Series	Hardware Models	Processor
Aruba 5400R Switch Series	5406R zl2 Switch (J9821A) 5412R zl2 Switch (J9822A) 5406R/5412R-24-port 10/100/1000Base-T PoE+ MACsec (No PSU) v3 zl2 Card (J9986A) 5406R/5412R-24p 1000BASE-T (No PSU) v3 zl2 Card (J9987A) 5406R/5412R-24p SFP (No PSU) v3 zl2 Card (J9988A) 5406R/5412R-12p PoE+ / 12p 1GbE SFP (No PSU) v3 zl2 Card (J9989A) 5406R/5412R-20p PoE+ / 4p SFP+ (No PSU) v3 zl2 Card (J9990A) 5406R/5412R-20p PoE+ / 4p 1/25/5/XGT PoE+ (No PSU) v3 zl2 Card (J9991A) 5406R/5412R-20p PoE+ / 1p 40GbE QSPF+ (No PSU) v3 zl2 Card (J9992A) 5406R/5412R-8p 1G/10GbE SFP+ v3 (No PSU) v3 zl2 Card (J9993A) 5406R/5412R-2-port 40GbE QSFP+ (No PSU) v3 zl2 Card (J9996A)	Freescale P2020 Dual Core

10 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 Assurance Activity Report for this evaluation, which is publicly available. 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 4 and CEM version 3.1 rev 4. The evaluation determined the Aruba 2930F, 2930M, 3810M, and 5400R Switch Series TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP20E.

10.1 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, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04 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.

10.2 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 NDcPP20E 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.

10.3 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.

10.4 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.

10.5 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 NDcPP20E 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.

10.6 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. The public search conducted on April 26, 2018 for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “HPE Aruba”, “3810M”, “2930F”, “2930M” “5400R”, “TCP”, “SSH”, “TLS” , “mocana” and “switch”.

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.

10.7 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.

11 Validator Comments/Recommendations

If an NTP server is used in the operational environment, the administrator of the product is encouraged to establish a trusted channel between the product and the NTP server.

Note that although the switches support features such as RIP, BGP, PoE+, those were not evaluated as part of this validation and no claims can be made, nor should any be inferred as to their integration and correct operation in the environment.

Administrators relying on auditing logs should be aware that the local audit log is a circular buffer and supports up to 6400 entries. Once the maximum number of entries is reached, the logs are overwritten without warning. If console logs are to be retained, administrators must manually transfer those console logs to the audit server.

12 Annexes

Not applicable

13 **Security Target**

The Security Target is identified as: *HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series (NDcPP20E) Security Target, Version 0.6, May 31, 2018*.

14 **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.

15 **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 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2102.

[4] collaborative Protection Profile for Network Devices, Version 2.0 + errata 20180314, 14 March 2018.

[5] HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series (NDcPP20E) Security Target, Version 0.6, May 31, 2018 (ST).

[6] Assurance Activity Report (NDcPP20E) for HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series, Version 0.4, May 31, 2018 (AAR).

[7] Detailed Test Report (NDcPP20E) for HPE Aruba 2930F, 2930M, 3810M, and 5400R Switch Series, Version 0.4, May 31, 2018 (DTR). <evaluation sensitive>

[8] Evaluation Technical Report for Aruba, a Hewlett Packard Enterprise Company 2930F, 2930M, 3810M, and 5400R Switch Series running ArubaOS version 16.04, Version 0.4, May 31, 2018 (ETR) <evaluation sensitive>

[9] Common Criteria Configuration Guidance, Network Device Collaboration Protection Profile, Target of Evaluation: Aruba 2930F, 2930M, 3810M and 5400R Switch Series, Version 1.4, May22, 2018 (AGD)