National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

Aruba Remote Access Point Version 6.5.0-FIPS

Report Number: CCEVS-VR-VID10766-2017
Dated: February 26, 2017
Version: 1.0

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

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the Aruba Remote Access Point Version 6.5.0-FIPS evaluation. It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Aruba Remote Access Point Version 6.5.0-FIPS was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in November 2016. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0138: IPsec VPN Client Testing of SPD Rules
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the Aruba Remote Access Point Version 6.5.0-FIPS Windows Endpoint is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) and associated test report produced by the Leidos evaluation team.

The TOE comprises software installed as an IPsec VPN client on an Aruba Remote Access Point. The TOE functions as an IPsec VPN client that enables the endpoint on which it is installed to establish an IPsec tunnel with an Aruba Master Controller. The TOE is evaluated on the following platforms; each containing a TPM:

- RAP-108 Remote Access Point (RAP-108-USF1, HPE SKU JW269A)
- RAP-109 Remote Access Point (RAP-109-USF1, HPE SKU JW275A)

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

Table 1: Evaluation Details

Item	**Identifier**
Evaluated Product	Aruba Remote Access Point Version 6.5.0-FIPS
Sponsor & Developer	Aruba, a Hewlett Packard Enterprise company 3333 Scott Blvd Santa Clara, CA 95054 United States
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	February 2017
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	*Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation: • TD0138: IPsec VPN Client Testing of SPD Rules • TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation • TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1 • TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4 • TD0037: IPsec Requirement_DN Verification
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the Aruba Remote Access Point Version 6.5.0-FIPS.
Evaluation Personnel	Dawn Campbell Cody Cummins
Validation Personnel	Sheldon Durrant Jean Petty

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) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	Aruba Remote Access Point Version 6.5.0-FIPS Security Target
ST Version	1.0
Publication Date	February 9, 2017
Vendor	Aruba, a Hewlett Packard Enterprise company
ST Author	Leidos
TOE Reference	Aruba Remote Access Point Version 6.5.0-FIPS
TOE Software Version	Version 6.5.0-FIPS
Keywords	IPsec VPN endpoint, VPN Client

2.1 Threats

The ST references the *Protection Profile for IPsec Virtual Private Network (VPN) Clients* to identify the following threats that the TOE and its operational environment are intended to counter:

- Failure to allow configuration of the TSF may prevent its users from being able to adequately implement their particular security policy, leading to a compromise of user information.
- Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- A user may gain unauthorized access to the TOE data. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- User data may be inadvertently sent to a destination not intended by the original sender because it is not rendered inaccessible after it is done being used.

2.2 Organizational Security Policies

The *Protection Profile for IPsec Virtual Private Network (VPN) Clients* does not identify any organizational security policies.

3 Architectural Information

The TOE is the Aruba Remote Access Point Version 6.5.0-FIPS which is the operating system and application engine for all Aruba controller-managed Remote Access Points (RAP). Designed for scalable performance, the TOE consists of three core components. First, a hardened, multicore, multithreaded supervisory kernel manages administration, authentication, logging and other system operation functions. This control plane is distinctly separate from the packet forwarding components to ensure continuous availability. Second, an embedded real-time operating system powers dedicated packet-processing hardware. This highly parallel architecture includes support for high-performance deep packet inspection of every connection that traverses the RAP, and implements all routing, switching and firewall functions. Third, a programmable encryption/decryption engine built on dedicated hardware delivers client-to-core encryption for wireless user data traffic and software VPN clients.

The claimed functionality for this evaluation is limited to the security functionality for a VPN client as claimed in the [VPNPP]. The security functionality specified in [VPNPP], includes protection of communications with the Aruba Master Controller, identification and authentication at the machine level when establishing the IPsec connection, ability to verify the source and integrity of updates to the TOE, specify client credentials and VPN gateways to use for connections, and specifies NIST-validated cryptographic mechanisms.

The TOE provided management functions are limited to specifying the IP address of the Aruba Master Controller, loading and managing certificates, and the identification of client credentials to be used for connections. Once the RAP is given the IP address of the Aruba Master Controller, it will bring up an IPsec tunnel using its factory-installed X.509 certificate (RSA2048/SHA1). When the RAP device boots it will establish a connection to its Aruba Master Controller and download its configuration file over a secure link. It can begin normal operation at this point, continuing to use the factory-installed certificate. All other management of the RAP is performed by the Aruba Master Controller.

Encryption and firewall policy can be configured and enforced from the IT department using profile based systems to insure uniformity. Troubleshooting can be performed on the packets entering the centralized location, and the RAP can be interrogated as to the state of connections and environmental conditions.

The Aruba Remote Access Point Version 6.5.0-FIPS allows users at any remote location equipped with a RAP to connect to an Aruba Master Controller over the Internet. These RAPs connect to the Aruba Master Controller using Layer-2 Tunneling Protocol and Internet Protocol Security (L2TP/IPsec) and send 802.11 data traffic through this tunnel. A secure RAP extends the corporate office to the remote site by giving remote users access to some of the same network features as corporate office users. They leverage the same access policies and service definitions used at headquarters or a branch office RAP deployment. Aruba Master Controllers act as VPN concentrators, eliminating the need for a parallel access infrastructure. For example, voice over IP (VoIP) applications can be extended to remote sites while the servers and the PBX remain secure in the corporate office.

The TOE implements NIST-validated cryptographic algorithms that support the IPsec protocols as well as digital signature services that support the secure update capabilities of the TOE. The encryption used to establish the secure IPsec VPN tunnel is provided by the TOE. Communication between the TOE and Aruba Master Controller uses the UDP 4500 port. IKE authentication can be configured to use digital certificates (RSA or ECDSA) to provide authentication.

4 Assumptions

The ST references the *Protection Profile for IPsec Virtual Private Network (VPN) Clients* to identify following assumptions about the use of the product:

- Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

4.1 Clarification of Scope

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

1. 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.
5. The following specific product capabilities are excluded from use in the evaluated configuration:
    a. Non-FIPS 140-2 mode of operation—this mode of operation allows cryptographic operations that are not FIPS-approved
6. The TOE is supported on the following platforms in its operational environment:
    - RAP-108 Remote Access Point (RAP-108-USF1, HPE SKU JW269A)
    - RAP-109 Remote Access Point (RAP-109-USF1, HPE SKU JW275A).

The TOE requires an Aruba Master Controller in its operational environment.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Cryptographic Support

The TOE is a FIPS certified cryptographic module: the ArubaOS 6.5.0-FIPS (cert #2182). The cryptographic module only employs FIPS-Approved DRBG, key generation, establishment, zeroization, encryption, digital signature, and hashing algorithms as specified by the FCS requirements.

5.2 User Data Protection

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

5.3 Identification and Authentication

Remote authentication for the TOE is provided by RSA or ECDSA certificate-based RAP provisioning. The TOE supports Distinguished Name (DN) peer identifiers for certificate-based peer authentication. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec sessions.

5.4 Security Management

The administrator may configure the TOE via a WebUI or CLI interface on the RAP to specify the IP address of the Aruba Master Controller, loading and managing certificates, and the identification of client credentials to be used for connections in order to establish an IPsec VPN connection.

The TOE is managed by an administrator via the Aruba Master Controller (i.e. the VPN Gateway) to configure the VPN tunnel and all security functions identified in this Security Target.

5.5 Protection of the TSF

The TOE provides self-tests to ensure the correct operation of the cryptographic functions and TSF hardware. The TOE verifies the integrity of stored TSF executable code when it is loaded for execution.

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

5.6 Trusted Path/Channels

The TOE initiates an IPsec tunnel with the remote Aruba Master Controller.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, there are four Common Criteria specific guides that reference the security-related guidance material for all products evaluated:

- *Aruba VPN Client Protection Profile, Common Criteria Configuration Guide Version 1.3, November 2016 [CC_CONFIG]*
- *ArubaOS 6.5.0.x User Guide, Revision 05, September 2016 [USER]*
- *ArubaOS 6.5.x Command-Line Interface Reference Guide, Revision 02, September 2016 [CLI]*.

Supporting TOE Guidance Documentation

- *Aruba Remote Access Point Version 6.5.0-FIPS Security Target*, v1.0, February 10, 2017

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Evaluation Team Test Report for Aruba Remote Access Point Version 6.5.0-FIPS, Version 1.0, February 09, 2017

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, with CSfC selections for VPN Clients applied. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:

- TD0138: IPsec VPN Client Testing of SPD Rules and is addressed in this ST
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, and the following NIAP Technical Decisions:

- TD0138: IPsec VPN Client Testing of SPD Rules and is addressed in this ST
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

The majority of Independent testing took place 8/1/2016 – 8/5/2016 at the HP/Aruba Facility in Littleton, MA. Additional test evidence was collected on 11/1/2016 and additional testing was performed remotely on 12/13/2016 (with NIAP approval).

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

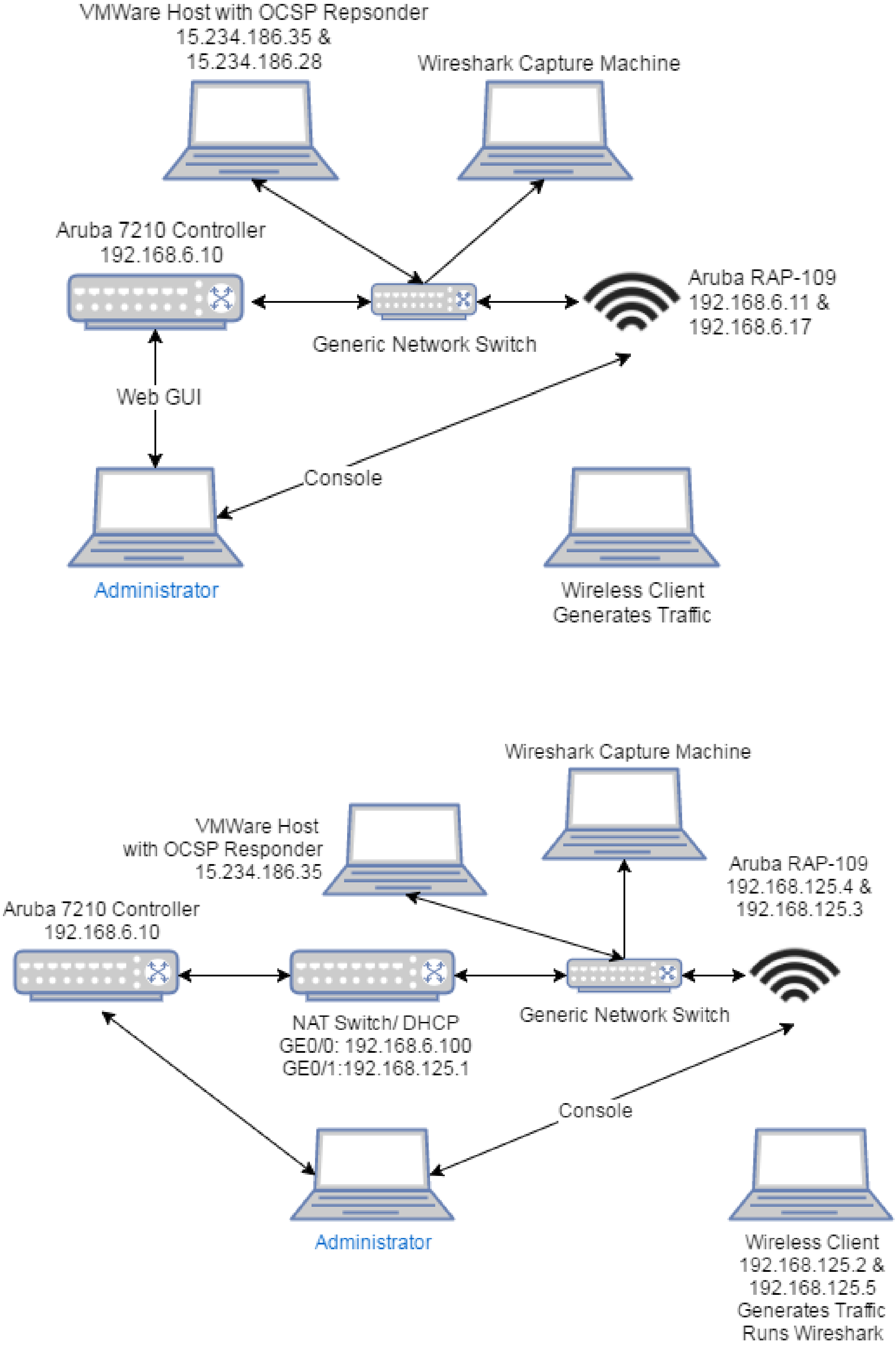

Figure 1: Configurations used for testing

As documented in the diagram above, the following hardware and software components were included in the evaluated configuration during testing:

- TOE Software
    - ArubaOS version 6.5.0-FIPS
- TOE Hardware Platform:
    - RAP-109 Remote Access Point (RAP-109-USF1, HPE SKU JW275A)
- Test Environment Components
    - VPN Gateway (Aruba 7210 Controller)
    - NAT Switch (HPE MSR 2003)
    - Network Packet Monitor (Wireshark)
    - Wireless Client connected to RAP
    - Administrator Device

As can be seen above, the configurations used during testing of the TOE match what was defined in the Security Target.

The evaluated version of the TOE was installed and configured according to the Aruba VPN Client Protection Profile, Common Criteria Configuration Guide Version 1.3, November 2016.

Given the complete set of test results from the test procedures were exercised by the evaluators, the testing requirements for the *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, and the following NIAP Technical Decisions are fulfilled:

- TD0138: IPsec VPN Client Testing of SPD Rules and is addressed in this ST
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- D0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification.

7.1 Penetration Testing

The evaluation team conducted an open source search for vulnerabilities in the product. The open source search did not identify any obvious vulnerabilities applicable to the TOE in its evaluated configuration.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in *Protection Profile for IPsec Virtual Private Network (VPN) Clients*, Version 1.4, 21 October 2013, and the following NIAP Technical Decisions:

- TD0138: IPsec VPN Client Testing of SPD Rules and is addressed in this ST
- TD0107: FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
- TD0079: RBG Cryptographic Transitions per NIST SP 800-131A Revision 1
- TD0053: Removal of FCS_IPSEC_EXT.1.12 Test 5 from VPN IPSEC Client v1.4
- TD0037: IPsec Requirement_DN Verification

in conjunction with version 3.1, revision 4 of the CC and the CEM. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Aruba VPN Client Protection Profile, Common Criteria Configuration Guide Version 1.3*, dated November 2016.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the product needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

10 Annexes

Not applicable

11 Security Target

- Aruba Remote Access Point Version 6.5.0-FIPS Security Target, v1.0, February 9, 2017

12 Abbreviations and Acronyms

Abbreviation	Description
CC	Common Criteria
CDP	CRL Distribution Point
PP	Protection Profile
SFR	Security Functional Requirement
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function(s)

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, 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 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Aruba Remote Access Point Version 6.5.0-FIPS Security Target, v1.0, February 9, 2017

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report For Aruba Remote Access Point Version 6.5.0-FIPS, Part 2 (Leidos Proprietary), Version 1.0, 10 February 2017