Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Aruba Networks Virtual Mobility Controller V6.4.2.0-1.3

Certification Report
2017/107

3-05-2017
Version 1.0

Amendment Record

Version	Date	Description
1.0	03-05-2017	External

Executive Summary

This report describes the findings of the IT security evaluation of Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Protected communications -** The TOE protects the communications to the WebUI using TLS/HTTPS, Command line interface (CLI) using SSHv2 and the Syslog, Radius and control plane security using IPSec.
- **Verifiable updates** - updates are digitally signed and verified upon installation utilising digital signatures.
- **System monitoring and audit –** The TOE maintains an audit log of administration and security relevant events. Logs can optionally be delivered to a Syslog server.
- **Secure administration –** The TOE provides administration interfaces for configuration and monitoring. The TOE authenticates administrators and implements session timeouts.
- **Residual information clearing** –The TOE ensures that network packets sent from the TOE do not include data "left over" from the processing of previous network information.
- **Self-test** – The TOE performs both power-up and conditional self-tests to verify correct and secure operation.
- **Firewall (**FWEP**)** –The TOE performs stateful packet filtering. Wireless clients connecting through APs are placed into user-roles. Stateful packet filter policies are applied to these user-roles to allow fine grained control over wireless traffic.
- **Virtual Private Network** (VPNGWEP) – TOE provides virtual private network (VPN) gateway functions. 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 network.

The report concludes that the product has complied with the Security Requirements for Network Devices Errata #3, version 1.1 (NDPP), Network Device Protection Profile Extended Package Stateful Traffic Filter Firewall version 1.0 (FWEP), and Network Device Protection Profile Extended Package VPN Gateway version 1.1 (VPNGWEP) and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC Australia and was completed on 31 March 2017.

With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Contents

Chapter 1 – Introduction

1.1 Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS against the requirements of the Common Criteria (CC), the NDPP v1.1, FWEP v1.0 and VPNGWEP v 1.1

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 1) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS
Software Version	6.4.2.0-1.3 FIPS
Hardware Platforms	• PacStar 451 Small Server Module (Intel 4th-Generation Core i5 or Core i7) • Information Assurance Specialists IAS Router MICRO Extreme network appliance (contains the IAS VPN Gateway Module CLASSIC using Intel 4th-Generation Core i5)

	• Klas Telecom Voyager VMm (Intel 5th-Generation Core i3) • DTECH Labs M3-SE-SVR3Q (Intel 3rd-Generation Core i7)
Security Target	Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS NDPP/TFFW-EP/VPNGW-EP Security Target 26 April 2017 v1.0
Evaluation Technical Report	Aruba Network Virtual Mobility Controller, Evaluation Technical Report (T0084) REFERENCE: CSC-EFC-T0084-ETR, Version 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, September 2012, Version 3.1.Rev 4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev 4
Conformance	NDPP v1.1 FWEP v1.0 VPNGWEP v1.1 Security Requirements for Network Devices Errata # 3
Developer	Aruba Networks 1344 Crossman Ave, Sunnyvale, CA 94089
Evaluation Facility	CSC Australia 12 Brindabella Circuit Brindabella Business Park ACT 2609

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS.

The Aruba Networks Virtual Mobility Controller (VMC) is a virtualised network device that serves as a gateway between wired and wireless networks and provides command-and-control over Access Points (APs) within an Aruba dependant wireless network. ArubaOS 6.4.2.0-1.3 FIPS is the underlying operating system of the VMC, which runs on top of VMware ESXi and was evaluated on the following hardware platforms:

a) PacStar 451 Small Server Module (Intel 4th-Generation Core i5 or Core i7)
b) Information Assurance Specialists IAS Router MICRO Extreme network appliance (contains the IAS VPN Gateway Module CLASSIC using Intel 4th-Generation Core i5)
c) Klas Telecom Voyager VMm (Intel 5th-Generation Core i3)
d) DTECH Labs M3-SE-SVR3Q (Intel 3rd-Generation Core i7)

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Protected communications -** The TOE protects the communications to the WebUI using TLS/HTTPS, Command line interface (CLI) using SSHv2and the Syslog, Radius and control plane security using IPSec.
- **Verifiable updates** – updates are digitally signed and verified upon installation utilising digital signatures.
- **System monitoring and audit –** The TOE maintains an audit log of administration and security relevant events. Logs can optionally be delivered to a Syslog server.
- **Secure administration –** The TOE provides administration interfaces for configuration and monitoring. The TOE authenticates administrators and implements session timeouts.
- **Residual information clearing** –The TOE ensures that network packets sent from the TOE do not include data "left over" from the processing of previous network information.

- **Self-test** – The TOE performs both power-up and conditional self-tests to verify correct and secure operation.
- **Firewall (FW EP)** –The TOE performs stateful packet filtering. Wireless clients connecting through APs are placed into user-roles. Stateful packet filter policies are applied to these user-roles to allow fine grained control over wireless traffic.
- **Virtual Private Network** (VPNGWEP) – TOE provides virtual private network (VPN) gateway functions. 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 network.

2.4 TOE Architecture

At a high level, the Aruba VMC is a 64-bit virtualised software-based WLAN, VPN, and firewall solution on x86 architecture. The VMC is the first hop for data traffic on virtualised network infrastructure. The VMC operates on x86 platforms in VMware environment and can reside with other virtualised appliances. The software running on the VMC is called ArubaOS, which consists of two main components:

- Control Plane (CP) - implements functions which can be handled at lower speeds such as VMC system management (CLI and Web GUI), user authentication (e.g. 802.1X, RADIUS, LDAP), 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 (GRE, IPsec), stateful firewall and deep packet inspection functions, and cryptographic acceleration. In the VMC, the Data Plane is implemented as a Linux process that makes use of the Intel Data Plane Development Kit (DPDK) framework.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per the Guidance (Ref 2).

The scope of the evaluation was limited to those claims made in the Security Target (Ref 1).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDDP (Ref 3), FWEP (Ref 4) and VPNGWEP (Ref 5) and sufficiently demonstrate the security functionality of the TOE.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 6) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

The following components are considered outside of the scope of the TOE:

- Access points
- Audit server
- Authentication server
- Time server
- Web Browser
- SSH Client
- VPN client
- IPsec for APs, VPN users and other mobility controllers is not within the scope of evaluation
- Operation in non-FIPS mode is not part of this evaluation.

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. This evaluation was performed against the U.S Government Protection Profile for Security Requirements for Network Devices (NDPP) Version 1.1, Errata #3, 3 November 2014, (Ref 3) the US Government Network Device Protection Profile (NDPP) Extended Package Stateful Traffic Filter Firewall (FWEP) Version 1.0, Dec 19, 2011(Ref 4) and the US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway (VPNGWEP), Version 1.1, 12 April 2013, therefore no Security Policy Model was provided for the TOE.

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS.

The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Guidance Documentation (Ref 2).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- For Software, the customer will access Aruba support portal to download images. Customers will be prompted for their login and password. Initial start-up procedures are detailed in the Guidance (Ref 2).

2.7.3 Installation of the TOE

The Configuration Guide (Ref 2) contains all relevant information for the secure configuration of the TOE.
The TOE performs both power-up and conditional self-tests to verify correct and secure operation. In the event that any self-test fails, the TOE will enter an error state, log the error, and reboot automatically. Failure of self-tests requires return to manufacturer.

2.8 Version Verification

For Software, the customer will access Aruba support portal to download images. Customers will be prompted for their login and password. Initial start-up procedures are detailed in Aruba Guidance (Ref 2).

Upgrade instructions are documented in the release notes for each software release, which will be posted in the same directory as the image file on the support portal. Upon successful verification, the TOE Administrators can update the TOE executable code using image files manually downloaded from the Aruba support portal. The administrator may perform an update from either the WebUI or CLI.
A SHA-256 hash of each update image is digitally signed using Aruba's code signing certificate (RSA 2048 bit). When an update is initiated, the TOE verifies the digital signature with a stored certificate (stored in Boot ROM). Upon successful verification, the TOE boots using the new image. Should verification fail, the TOE will enter into an error state. The TOE's error state will allow direct console access only, where an administrator can change to a new file partition or TFTP a new image and re-boot.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased.

- ArubaOS 6.4.2 User Guide, Ref 0511615-00v1
- ArubaOS 6.4.2 Command Line Interface, Ref 0511616-00v1
- ArubaOS 6.4. Syslog Messages Guide, Ref 0511324-02

- ArubaOS 6.x MIB Reference Guide, Ref 0511323-02
- Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy

All guidance material is available for download at **https://support.arubanetworks.com/**. All common criteria guidance material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met. The assumptions are identical to those of the NDPP, TFFW-EP and VPNGW-EP.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDPP (Ref 4), FWEP (Ref 5), VPNGWEP (Ref 6), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 7 and 8).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 12).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from configuration guidance (Ref 2).

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the Evaluators were taken from the NDPP, FWEP and VPNGWEP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.3.2 Test phases

Testing is determined in the assurance activities in the Protection Profiles. The evaluators conducted independent and penetration testing between the 21st October 2016 and 25th of October 2016, and 15 Feb 2017 to 16 Feb 2017.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 11).

3.5 Penetration Testing

The Evaluator performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time)

b) Specialist technical expertise required (specialist expertise)

c) Knowledge of the TOE design and operation (knowledge of the TOE)

d) Window of opportunity

e) IT hardware/software or other equipment required for the exploitation.

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the Certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with the Protection Profile and associated Extended Packages that cover the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the Certifiers and of the Evaluation Technical Report (Ref 9) the Australasian Certification Authority **certifies** the evaluation of the Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS performed by the Australasian Information Security Evaluation Facility, CSC Australia.

The AISEF **has determined** that TOE upholds the claims made in the Security Target (Ref 1) and **has met** the requirements of the NDPP, the FWEP and the VPNGWEP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles.

The analysis is supported by testing as outlined in the NDPP, FWEP and VPNGWEP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.4 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 6) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved.

Annex A – References and Abbreviations

A.1 References

1. Aruba Networks Virtual Mobility Controller (hardened Chassis running VMware ESXi) with ArubaOS 6.4.2.0-1.3 FIPS Security Target 26 April 2017 v1.0

2. Guidance Documentation:

   - ArubaOS 6.4.2 User Guide, Ref 0511615-00v1
   - ArubaOS 6.4.2 Command Line Interface, Ref 0511616-00v1
   - ArubaOS 6.4. Syslog Messages Guide, Ref 0511324-02
   - ArubaOS 6.x MIB Reference Guide, Ref 0511323-02
   - Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy

3. U.S Government Protection Profile for Security Requirements for Network Devices (NDPP) Version 1.1, Errata #3, 3 November 2014

4. US Government approved Network Devices Protection Profile – Protection Profile Stateful Traffic Filter Firewall Extended Package (FWEP) Version 1.0 December 2011

5. US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNGWEP)

6. 2016 Australian Government Information Security Manual (ISM), Australian Signals Directorate

7. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components 09- 2012, Version 3.1 Revision 4

8. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components 09- 2012, Version 3.1 Revision 4

9. Aruba Network Virtual Mobility Controller Evaluation Technical Report (T0084) REFERENCE: CSC-EFC-T0084-ETR Version 1.0 dated 11 April 2017

10. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

11. Aruba VMC Tactical Entropy Documentation 16-01- 2017 Version 1.6

12. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, 09 - 2012, Version 3.1, Revision 4.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certification Authority
CC	Common Criteria
CEM	Common Evaluation Methodology
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SNMP	Secure Network Management Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy