Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Aruba Networks Mobility Controller

Certification Report
2016/94

11 February 2016
Version 1.0

Amendment Record

Version	Date	Description
1.0	11-02-2016	Final

Executive Summary

This report describes the findings of the IT security evaluation of Aruba Networks Mobility Controller v6.4.3.4 against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Aruba Networks Mobility Controller. The TOE is a product that is a 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.

The functionality defined in the Security Target (Ref 1) that was subsequently evaluated is summarised as follows:

- **WebUI -** Communication with the administrative web user interface (WebUI) is protected using TLS/HTTPS
- **Protection of the TSF** - The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **CLI -** Remote administration via the Command Line Interface (CLI) is protected using SSHv2
- **Syslog -** Syslog messages are protected using IPSec
- **TOE Access** - The TOE can be configured to terminate inactive sessions
- **Radius -** Radius authentication messages are protected using IPSec
- **Verifiable updates -** Updates are digitally signed and verified upon installation utilising digital signatures
- **System monitoring -** The TOE maintains an audit log of administrative and security relevant events. Logs can optionally be delivered to a Syslog server
- **Secure communication** - with remote administrators, authentication servers and audit servers
- **Trusted Path / Channels** - The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator
- **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
- **Stateful Traffic Filtering** (FWEP & VPNGWEP) - TOE provides stateful network traffic 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 Gateway** (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 or untrusted network
- **Self verification of integrity and operation -** The TOE performs both power-up and conditional self-tests to verify correct and secure operation.

The report concludes that the product has complied with the Security Requirements for Network Devices, 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 17 November 2015.

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
d) By default, the TOE enables the FTP service for the purpose of providing software images to wireless access points. This service should be disabled when operating in an approved mode of operation. To disable the FTP service, use the CLI command "firewall disable-ftp-server"
e) Aggressive mode must be disabled in order to ensure it is not used. This is documented in ArubaOS 6.4.3.X Command Line Interface (Ref 2) and is performed using the command "crypto-local isakmp disable-aggressive-mode".

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.

Table of 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 Mobility Controller v6.4.3.4-FIPS against the requirements of the Common Criteria (CC), the NDPP v1.1, and 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 Mobility Controller (7240, 7220, 7210, 7030, 7205, 7024, 7010, 7005, 6000, 3600, 3400, 3200, 650 and 620) with ArubaOS 6.4.3.4-FIPS, software Version: 6.4.3.4-FIPS.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	Aruba Networks Mobility Controller v6.4.3.4-FIPS
Software Version	6.4.3.4-FIPS
Hardware Platforms	Aruba 7000 Series Mobility controller. (7240, 7220, 7210, 7205, 7030, 7024, 7010, 7005) Aruba 6000 Series. The Aruba 6000 with M3 blades are designed for corporate headquarters and large campus deployments.

	Aruba 3000 Series. The Aruba 3200, 3400 and 3600 are designed for small, medium and large enterprises. Aruba 600 Series. The Aruba 620 and 650 are designed for branch offices and similar deployments.
Security Target	Aruba Networks Mobility Controller (7240, 7220, 7210, 7030, 7205, 7024, 7010, 7005, 6000, 3600, 3400, 3200, 650 and 620) with ArubaOS 6.4.3.4-FIPS NDPP/TFFW-EP/VPNGW-EP Security Target, v1.5 18 January 2016
Evaluation Technical Report	Aruba Network Mobility Controller Evaluation Technical Report (T0079) REFERENCE: CSC-EFC-T0079-ETR Version 1.0 20-01-2016
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 Public Sector Certifications 1344 CROSSMAN AVE SUNNYVALE CA 94089 USA
Evaluation Facility	Computer Science Corporation Australia (CSC) 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 a network device, stateful traffic filter firewall and VPN gateway. It is a product 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.

2.3 TOE Functionality

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

- **Secure management -** including authentication, verifiable updates and auditing
- **WebUI -** Communication with the administrative web user interface (WebUI) is protected using TLS/HTTPS
- **Protection of the TSF** - The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords.
- **CLI -** Remote administration via the Command Line Interface (CLI) is protected using SSHv2
- **Syslog -** Syslog messages are protected using IPSec
- **TOE Access -** The TOE can be configured to terminate inactive sessions
- **Radius -** Radius authentication messages are protected using IPSec
- **Verifiable updates -** Updates are digitally signed and verified upon installation utilising digital signatures
- **System monitoring -** The TOE maintains an audit log of administrative and security relevant events. Logs can optionally be delivered to a Syslog server
- **Secure communication** - with remote administrators, authentication servers and audit servers
- **Trusted Path / Channels** - The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator
- **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

- **Stateful Traffic Filtering** (FWEP & VPNGWEP) - TOE provides stateful network traffic 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 Gateway** (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 or untrusted network
- **Self verification of integrity and operation** - The TOE performs both power-up and conditional self-tests to verify correct and secure operation.

2.4 TOE Architecture

The TOE consists of the following major subsystems:

a) **ArubaOS 6.4.3.4-FIPS software.**

The Aruba OS 6.4.3.4-FIPS consists of a base software package with add on software modules that can be activated by installing the appropriate licenses

b) **Aruba Models.**

The difference in the models includes the physical appearance, number of ports, interfaces, throughput and processing speed.

Model	Maximum Access points	Throughput	Maximum users
7240	2048	40Gbs	65,536
7220	1024	40Gbs	32,768
7210	512	28.3Gbs	16,384
7030	64	8 Gbps	4096
7205	128	20Gbps	8192
7024	32	TBD	2048
7010	32	4	2049
7005	16	2Gbs	1024
6000 with four M3 blades	2048	80Gbs	32,768
3600	128	4Gbs	8,192
3400	64	4Gbs	4,096
3200	32	3Gbs	2,048
650	16	2Gbs	512
620	8	800Mbs	256

Table 2: TOE Chassis and appliance numbers

Aruba mobility controllers are hardware appliances consisting of a multicore network processor, Ethernet interfaces and required supporting circuitry and power supplies enclosed in a metal chassis. The software running on the Mobility Controller is called ArubaOS which consists of two main components, the control plane (CP) and the data plane (DP), both implemented on multiple cores within a single processor. The Control Plane which implements functions which can be handled at a lower speeds such as the Mobility Controller system management, user authentication, internet key exchange and audit logging. The control plane runs the Linux operating system along with various user space applications.
Data Plane implements functions that must be handled at high speeds such as switching functions (forwarding, VLAN Tagging/enforcement, bridging) termination of 802.11 associations/sessions, tunnel termination (IPsec) and deep packet inspection functions and cryptographic acceleration. The data plane runs a lightweight, propriety real-time OS which is known as "SOS" The Control Plane and Data plane are inseparable. The Control Plane provides the following functions:

a) Monitors and manages critical system resources , including processes, memory and flash
b) Manages system configuration and licensing
c) Manages an internal data base used to store licenses and user authentication information
d) Provides network anomaly detection, hardware monitoring, mobility management, wireless management and radio frequency management services
e) Provides a Command Line Interface
f) Provides a web based (HTTPs/TLS) management UI for the mobility controller
g) Provides authentication services for the system management interfaces and
h) Provides Syslog services by sending logs to the operating environment.

Administrators do not have access to the Linux command shell or operating system.

The data plane is further subdivided into two subcomponents: Fast Path and Slow Path. The Fast Path implements high speed packet forwarding and sends packets to the Slow Path.

The data plane is implemented on a multi-core processor. The SOS contains an Ethernet Driver, a serial driver, a logging facility, semaphore support, and a crypto driver. In the Aruba 6000 with M3 controller card, an FPGA is also used to control and monitor the switch fabric, Ethernet interface hardware and provide security functionality such as filtering.

The DP and CP run on different hardware platforms but the security functionality remains the same, regardless of the model. The difference in the platforms is in the processors, memory capacity, physical interfaces and FPGA implementation. These differences are based on performance and scalability requirements.

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 documentation (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 NDPP (Ref 3), FWEP (Ref 4) and VPNGWEP (Ref 5) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

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.** APs connect to the TOE in Aruba dependent wireless network architectures. Wireless clients connect to the APs
- **Audit Server.** The TOE can utilize a Syslog server to store audit records
- **Authentication Server.** The TOE can utilize a Radius server to authenticate users
- **Time Server.** The TOE can utilize a Network Time Protocol (NTP) server to synchronize its system clock with a central time source
- **Web Browser.** The remote administrator can use a web browser to access the Web GUI interface
- **SSH Client.** The remote administrator can use an SSH client to access the CLI
- **VPN Client.** When acting as a VPN gateway, the TOE may communicate with other VPN gateways or with VPN clients. The VPN clients may be hardware devices (e.g. Aruba Remote Access Point) or may be implemented as software (e.g. Aruba VIA Client).

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 7), the US Government Network Device Protection Profile

(NDPP) Extended Package Stateful Traffic Filter Firewall (FWEP) Version 1.0, Dec 19, 2011 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 software version: 6.4.3.4-FIPS and Aruba appliance models: 7240, 7220, 7210, 7030, 7205, 7024, 7010, 7005, 6000, 3600, 3400, 3200, 650 and 620. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the guidance (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 Security Target (Ref 1).

The hardware units are shipped to the in factory-sealed boxes using trusted commercial carrier shipping companies. They should be examined for evidence of tampering. Tamper-evidence includes tears, scratches, and other irregularities in the packaging. Details are available in Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy & Aruba 7XXX Series Controllers FIPS 140-2 Security Policy (Ref 2).

2.7.3 Installation of the TOE

The guidance (Ref 2) contains all relevant information for the secure configuration of the TOE. It should be noted that some well-known protocols are prevented from operating as per the FWEP. Network design should take this into account.

2.8 Version Verification

The verification of the TOE is by the “Show version” command.

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. 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.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE

- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment
- Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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 3), FWEP (Ref 4), VPNGWEP (Ref 5), Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4, Parts 2 and 3 (Ref 8 and 9).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 10).

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 (Ref 11) were also upheld.

The evaluation was based on the default installation and configuration of the TOE with additional configuration taken from the guidance (Ref 2). Results were recorded on worksheets (Ref 12).

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. The evaluators conducted independent and penetration testing between the 20th October 2015 and the 6th of November 2015.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 13).

3.5 Penetration Testing

The developer 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 evaluators performed a search for public domain vulnerabilities for the specific Models of the Aruba Controller and similar devices. The analysis also covered generic vulnerabilities including the protocols utilised by the TOE and vulnerabilities identified in all evaluation documentation. Based upon the evaluator's vulnerability analysis, the evaluators developed and executed penetration tests. As a result of testing the evaluators determined that the TOE is resistant to the vulnerabilities identified and to penetration attacks performed by an attacker possessing a Basic attack potential.

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 a Protection Profile that covers 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.

The analysis is supported by testing as outlined in the NDPP, FWEP and VPNGWEP assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

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 14) the Australasian Certification Authority **certifies** the evaluation of the Aruba Networks Mobility Controller v6.4.3.4-FIPS product performed by the Australasian Information Security Evaluation Facility, CSC Australia.

CSC Australia **has determined** that Aruba Networks Mobility Controller v6.4.3.4-FIPS uphold the claims made in the Security Target (Ref 1) and **has met** the requirements of the NDPP, FWEP and 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.
d) By default, the TOE enables the FTP service for the purpose of providing software images to wireless access points. This service should be disabled when operating in an approved mode of operation. To disable the FTP service, use the CLI command "firewall disable-ftp-server".
e) Aggressive mode must be disabled in order to ensure it is not used. This is documented in CLI guidance and is performed using the command "crypto-local isakmp disable-aggressive-mode".

Annex A – References and Abbreviations

A.1 References

1. Security Target – Aruba Networks Mobility Controller (7240, 7220, 7210, 7030, 7205, 7024, 7010, 7005, 6000, 3600, 3400, 3200, 650 and 620) with ArubaOS 6.4.3.4-FIPS NDPP/TFFW-EP/VPNGW-EP Security Target, Version 1.5, 18 Jan 2016

2. Guidance Documentation:

   a) ArubaOS 6.4.X Quick Start Guide, Ref 0511696-03

   b) ArubaOS 6.4.3.X User Guide, ref 0511693-00v2

   c) ArubaOS 6.4. Syslog Messages Guide, Ref 0511324-05

   d) ArubaOS 6.4.3.X Command Line Interface, Ref 0511694-00v2

   e) ArubaOS 6.4.3.4 Release Notes, Ref 0511695-04v2

   f) Aruba 600/3000/6000/7200 FIPS 140-2 Security Policy &

   g) Aruba 7XXX Series Controllers FIPS 140-2 Security Policy

3. US Government approved Protection Profile – Security Requirements for Network Devices (NDPP) version 1.1, 8 Jun 2012

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. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

7. The US Government Network Device Protection Profile (NDPP) Errata #3, 3 November 2014,

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

9. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components September 2012, Version 3.1 Revision 4

10. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2012, Version 3.1, Revision 4

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

12. Test Documentation

    - CSC-EFC-T079-WS-CMC 1.0 2015
    - CSC-EFC-T079-WS- NDPP-TFFW-VPNGW_ST 3.0 2015
    - CSC-EFC-T079-WS- NDPP-IND 2.0 2015
    - CSC-EFC-T079-WS- OPE 2.0 2015
    - CSC-EFC-T079-WS- PRE 1.0 2015
    - CSC-EFC-T079-WS- VAN 2.0 2015

13. Aruba Mobility Controller Entropy Documentation v1.3, 6 Nov 2013

14. Aruba Network Mobility Controller Evaluation Technical Report (T0079) REFERENCE: CSC-EFC-T0079-ETR, Version 1.0, 20 Jan 2016

15. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

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
CLI	Command line interface
CEM	Common Evaluation Methodology
CP	Control Plane
DP	Data Plane
ETR	Evaluation Technical Report
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
NTP	Network Time Protocol
NDPP	U.S. Government Approved Protection Profile - Security Requirements for Network Devices, v1.1 with Errata #3
FWEP	US Government approved Network Devices Protection Profile – Protection Profile Stateful Traffic Filter Firewall Extended Package Version 1.0 December 2011
VPNGWEP	US Government Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 (VPNGWEP)
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
UI	User Interface