Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

HPE Aruba Networking Orchestrator and EdgeConnect Release 9.4.2

Version 1.1, 14 March 2025

Document reference: AISEP-CC-CR-2025-EFT-T049-CR-V1.1
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of HPE Aruba Networking Orchestrator and EdgeConnect Release 9.4.2 against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is a distributed network device that provides VPN Gateway and Firewall capabilities.

HPE Aruba Networking Orchestrator is deployed as an on-premises virtual appliance to monitor and manage one or more EdgeConnects. EdgeConnect devices are deployed on the network edge as gateway devices providing firewall and VPN services. The EdgeConnect devices communicate between each other via VPN tunnelling.

This report concludes that the Target of Evaluation (TOE) has complied with the following PPs [4]:

- Collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 (CPP_ND_V2.2E)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 (MOD_CPP_FW_V1.4e)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, 16-August-2023 (MOD_VPNGW_V1.3)

Additionally, the above PPs are combined and evaluated as a whole under the following PP-configuration [4]:

- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version: 1.3, 2023-08-18 (CFG_NDcPP-FW-VPNGW_V1.3)

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP) [10]. The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 18 February 2025.

With regard to the secure operation of the TOE, the Australian Certification Authority recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.hpe.com/ website
- the system auditor should review the audit trail generated and exported by the TOE periodically.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

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.

Introduction

Overview

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

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [1, 2, 3] and Protection Profiles [4]
- provide a source of security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [7] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is HPE Aruba Networking Orchestrator and EdgeConnect Release 9.4.2

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	HPE Aruba Networking Orchestrator and EdgeConnect Release 9.4.2
Software version	Release 9.4.2
Hardware platforms	EdgeConnect
Security Target	HPE Aruba Networking Orchestrator and EdgeConnect Release 9.4.2 Security Target, Version 1.16, 14 March 2025
Evaluation Technical Report	Evaluation Technical Report - HPE Aruba Networking orchestrator and Edge Connect Release 9.4.2, dated 18 February 2025
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5

Conformance	collaborative Protection Profile for Network Devices, Version 2.2e, 23-March-2020 (CPP_ND_V2.2E) PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25-June-2020 (MOD_CPP_FW_V1.4e) PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3, 16-August-2023 (MOD_VPNGW_V1.3) PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.3, 18-August-2023 (CFG_NDcPP-FW-VPNGW_V1.3)
Developer	Hewlett Packard Enterprise
Evaluation facility	Teron Labs Unit 3, 10 Geils Court Deakin ACT 2600 Australia

Target of Evaluation

Overview

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

Description of the TOE

HPE Aruba Networking EdgeConnect provides SD-WAN, firewall, segmentation, routing, WAN optimization and application visibility and control in one centrally managed platform. Aruba Orchestrator provides management of EdgeConnect appliances giving enterprises the ability to centrally assign policies to secure and control applications across the WAN.
Orchestrator is deployed as an on-premises virtual appliance to monitor and manage one or more EdgeConnects. EdgeConnect devices are deployed on the network edge as gateway devices providing firewall and VPN services. The Orchestrator manages one or more EdgeConnect devices and EdgeConnect devices communicate between each other via VPN tunnelling.

TOE Functionality

The TOE functionality that was evaluated is described in section 2 of the Security Target [7].

TOE Physical Boundary

The TOE boundary includes an EdgeConnect hardware appliance component and an Orchestrator virtual appliance component:

- The EdgeConnect Release 9.4.2 component consists of the EdgeConnect EC-XS Model 500210 which is equipped with the Intel® Atom C3558, 2.20 GHz, 4C/4T (Denverton) CPU, running the ECOS 9.4.2 on Yocto 2.7.3 Warrior with Kernel 4.19.87

- The Orchestrator Release 9.4.2 virtual appliance component consists of the Orchestrator 9.4.2 OVA software running on Rocky Linux 5.14.0.

The Orchestrator component is classified as a virtual network device (vND) corresponding to evaluated configuration Case 1 of Section 1.2 of CPP_ND_V2.2E. As such, the TOE boundary comprises the virtual machine (VM) software, but excludes the virtual system (hypervisor and hardware platform). The Orchestrator VM operates on the hypervisor VMware ESXi 7.0. For the evaluation, it was tested on a HPE ProLiant DL360 hardware platform. The table below shows the details on the evaluated configuration of the TOE.

Component	HW Model	CPU	Software
EdgeConnect Release 9.4.2	EdgeConnect EC-XS Model 500210, P/N 201571	Intel® Atom C3558, 2.20 GHz, 4C/4T (Denverton)	ECOS 9.4.2 on Yocto 2.7.3 Warrior (4.19.87 Kernel)

Orchestrator Release 9.4.2	HPE ProLiant DL360	Intel Xeon-Gold 6242R (3.1GHz/20-core/205W) FIO Processor Kit for HPE ProLiant DL360 Gen10 (Cascade Lake)	Orchestrator 9.4.2 OVA on Rocky Linux 5.14.0 on VMware ESXi 7.0

Architecture

The TOE architecture embodies a distributed network device designed to provide robust VPN Gateway and Firewall capabilities. This architecture comprises two primary components. The Aruba Networking Orchestrator and the EdgeConnect devices. The Orchestrator, deployed as an on-premises virtual appliance, functions as the central authority for orchestrating, monitoring, and managing multiple EdgeConnect devices. The EdgeConnect devices operate as network-edge gateway entities, delivering advanced security services, including firewall protection and encrypted VPN connectivity. These devices facilitate seamless and secure intercommunication via cryptographically fortified VPN tunnels, ensuring data integrity, confidentiality, and resilience against cyber threats.

The TOE framework is underpinned by a suite of management and operational interfaces, which is described below in Figure 1. It is designed to provide security and administrative efficiency. The Orchestrator component is accessible through a Command Line Interface (CLI) via SSH, a web-based Graphical User Interface (GUI) fortified with HTTPS encryption, and auxiliary interfaces dedicated to log transmission (Syslog), time synchronisation (NTP), and inter-component communication via TLS. Correspondingly, EdgeConnect devices incorporate similar interfaces, enabling secure remote administration, event logging, and cryptographically authenticated time updates. The communication pathways between the Orchestrator and EdgeConnect devices are safeguarded by advanced encryption protocols, such as TLS and IPsec, thereby enhancing network security and operational integrity.

The architecture enforces protected communication, secure administrative controls through role-based access control policies and configurable authentication measures, and the deployment of trusted software updates validated through cryptographic signatures. Additionally, it incorporates system monitoring through logged security-relevant events, supporting forensic analysis and compliance auditing. Cryptographic operations, underpinned by validated cryptographic libraries, further enhance the security posture of the TOE, safeguarding both network traffic and administrative functions. The physical scope of the TOE encompasses the EdgeConnect hardware appliance and the Orchestrator virtual appliance, operating within defined hardware and software environments, ensuring optimal reliability, scalability, and enterprise-grade security.

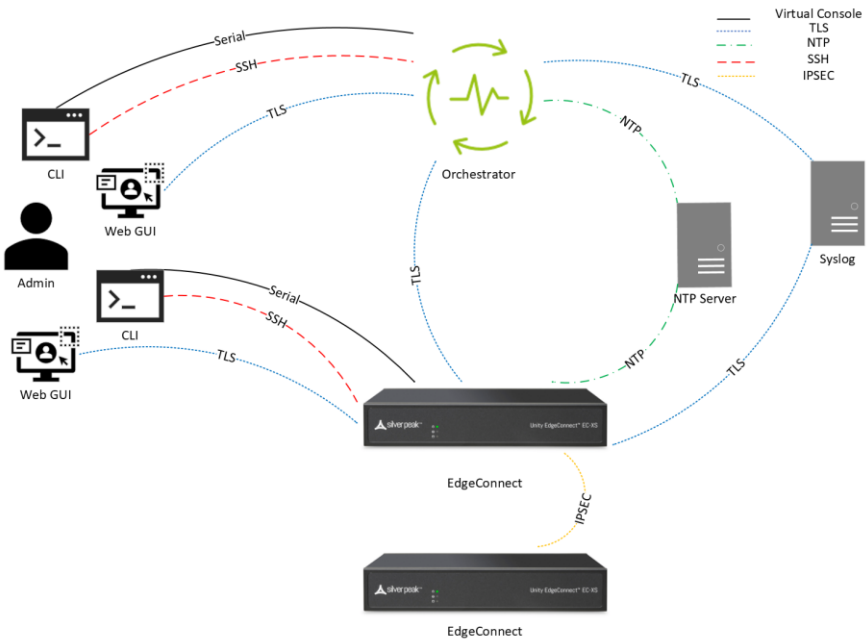

Figure 1

The TOE interfaces are as follows:

a) Orchestrator CLI, command line management interface via virtual console or remote SSH

b) Orchestrator Web GUI, HTTPS Web management interface via TLS

c) Orchestrator Syslog, transmission of logs to a remote server via TLS

d) Orchestrator NTP time updates via NTP

e) Orchestrator to EdgeConnect. Inter TOE management connection via TLS

f) EdgeConnect CLI, command line management interface via serial console or remote SSH

g) EdgeConnect Web GUI, HTTPS Web management interface via TLS

h) EdgeConnect Syslog, transmission of logs to a remote server via TLS

i) EdgeConnect NTP, time updates via NTP

j) EdgeConnect VPN Tunnel, encrypted VPN tunnel between EdgeConnects via IPsec.

Clarification of Scope

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

The scope of the evaluation was limited to those claims made in the Security Target [7].

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profiles [4] and Supporting Documents [12] and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE operates with the following components in the environment:

a) Audit Server, the TOE sends audit events to the remote syslog server

b) NTP Server, Network Time Protocol server

c) Non-EdgeConnect VPN Peer, any VPN device which is not an EdgeConnect that may connect to the EdgeConnect TOE component

d) VMware hypervisors (ESX, ESXi, vSphere), the Orchestrator operates on VMware ESXi 7.0

e) Management station, computer used to connect to the Orchestrator and EdgeConnect for management operations.

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 the Australian Government Information Security Manual [5] for policy relating to using an evaluated product in an unevaluated configuration.

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

a) Rest API

Security

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [7] contains a summary of the functionality that is evaluated.

Secure Delivery

Obtaining the TOE

The TOE hardware is delivered by commercial courier. The TOE software is downloaded to a local machine from the vendor website and then loaded on to the TOE.

It is highly recommended that the TOE hardware be sourced from HPE's official website hpe.com

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform:

- Shipping label – Verify the shipping label reflects the receiver's name and address, as well as identifying the device inside.
- outside packaging - Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device
- inside packaging - Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, they should immediately contact the supplier providing the order number, tracking number and a description of the identified problem to the supplier.

Installation of the TOE

The Configuration Guides [6] contains all relevant information for the secure configuration of the TOE.

Version Verification

The verification of the TOE is largely automatic, as demonstrated in testing. The TOE cannot load a modified software image. Authentic software images can be downloaded from hpe.com. In addition to the automated verification, the site includes individual hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform

The current version of the Orchestrator can be queried from the Web GUI in the top right corner of the UI.

The current version and recently installed version of EdgeConnect appliances can be queried from the Orchestrator UI via Administration=>Software=>Upgrade=>Software Versions page or by executing show image via the CLI.

EdgeConnect appliances have two software partitions which allows a current running partition (in the active version) and either a prior image or a newer image in the other partition (inactive partition). In Orchestrator, navigate to Administration=>Software=>Upgrade=>System Information.

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. The evaluated configuration guide (System Admin Guide) document for the HPE Aruba Networking orchestrate and edge connect release 9.4.2 is available for download at https://www.arubanetworks.com/techdocs/sdwan/ The title is:

- *HPE Aruba Networking EdgeConnect SD-WAN Common Criteria Guidance, Orchestrator and ECOS Version 9.4.2, Version 1.3.4, December 2024*

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5].

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 network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

The administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organisation. This includes being appropriately trained, following policy and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known security vulnerabilities.

The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

The administrator must ensure that there is no unauthorised access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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.

Evaluation

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.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant Protection Profiles [4] and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].

Testing methodology was drawn from Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3], the relevant Supporting Documents [12].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9] and the document CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs [13] were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the Protection Profiles [4] and Supporting Documents [12]. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [11]. CAVP certificate references, organised by the applicable Security Functional Requirements, are given in the Security Target [7].

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12.a] and FW_MOD Supporting Document [12.b] which follow a flaw hypothesis methodology. This effort also met the requirements for the MOD_VPNGW Supporting Document [12.c]. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - ND-iTC (Network international Technical Community) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the **18 February 2025** coinciding with the conclusion of the evaluation. There were no identifiable Type 2 hypotheses for this evaluation.

The evaluation team devised three tests to check for potential vulnerabilities.

- Within the TOE's boot process
- For web objects easily accessible in the TOE's web server
- Through a protocol scan, the evaluators verified the TOE was resistant to a certain DoS attack.

The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12]. Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

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

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of network devices with added security functionality including stateful traffic firewall functions and VPN gateway functions. Organisations 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 threats will have been addressed.

The analysis is supported by testing as outlined in the PP Supporting Documents, Protection Profile Module 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.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles [4]. PPs provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [7] and **has met** the requirements of the Protection Profiles NDcPP V2.2e [4.a], FW_MOD [4.b], MOD_VPNGW [4.c], and CFG_NDcPP-FW-VPNGW_V1.3 [4.d].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australian Certification Authority **certifies** the evaluation of the HPE Aruba Networking orchestrator and Edge Connect Release 9.4.2 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [7] claim to have met the requirements of the relevant protection profiles [4].

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the Australian Government Information Security Manual [5].

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

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood

- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.hpe.com/ website
- the system auditor should review the audit trail generated and exported by the TOE periodically

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. Protection Profiles:
    a) *collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020*
    b) *PP-Module for Stateful Traffic Filter Firewalls* + Errata 20200625 *(*MOD_CPP_FW*), Version 1.4, 25 June 2020*
    c) *PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), version 1.3, 16 August 2023*
    d) *PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version: 1.3, 2023-08-18 (CFG_NDcPP-FW-VPNGW_V1.3)*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. Guidance documentation:
    a) *HPE Aruba Networking EdgeConnect SD-WAN Common Criteria Guidance, Orchestrator and ECOS Version 9.4.2, Version 1.3.4, December 2024*
7. *Security Target for HPE Aruba Networking orchestrator and Edge Connect Release 9.4.2, Version 1.16, 14 March 2025*
8. *Evaluation Technical Report - HPE Aruba Networking orchestrator and Edge Connect Release 9.4.2, dated 18 February 2025*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf
11. Entropy Documentation:
    a) *HPE Aruba Networking Aruba Jitter Implementation Entropy Assessment and SP 800-90B Compliance Report, Version 1.02, November 17, 2023.*
12. Protection Profile Supporting Documents

a) *Supporting Document, Evaluation Activities for Network Device cPP, September 2018, version 2.1 (NDcPP-SD)*

b) *Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, September 2019, Version 1.3 (FW_MOD-SD)*

c) *Supporting Document, Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Gateways, version 1.0, dated 2019-09-17, (MOD_VPNGW_SD)*

13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
CLI	Command Line Interface
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
GUI	Graphical User Interface
HPE	Hewlett Packard Enterprise
HTTPS	Hypertext Transfer Protocol Secure
IPsec	Internet Protocol Security
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
ND-iTC	Network international Technical Community
NTP	Network Time Protocol
PIN	Personal Identification Number
PP	Protection Profile
SD-WAN	Software-Defined Wide Area Network
SFR	Security Functional Requirements

SSH	Secure Shell
ST	Security target
TLS	Transport Layer Security
TOE	Target of Evaluation
UI	User Interface
VM	Virtual Machine
vND	Virtual Network Device
VPN	Virtual Private Network
WAN	Wide Area Network

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate