National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

HPE Aruba Networking ClearPass Policy Manager 6.11

Report Number: **CCEVS-VR-VID11548-2025**

Dated: **April 29, 2025**

Version: **1.0**

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

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Swapna Katikaneni
Marybeth Panock
Mike Quintos
The Aerospace Corporation

Common Criteria Testing Laboratory

Douglas Kalmus
Matai Spivey
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of HPE Aruba Networking ClearPass Policy Manager 6.11 solution provided by HPE Aruba Networking. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in April 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e) with the Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10).

The Target of Evaluation (TOE) is the HPE Aruba Networking ClearPass Policy Manager 6.11.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the HPE Aruba Networking ClearPass Policy Manager 6.11 Security Target, version 1.0, April 15, 2025 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	HPE Aruba Networking ClearPass Policy Manager 6.11 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e) with the Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10)
ST	HPE Aruba Networking ClearPass Policy Manager 6.11 Security Target, version 1.0, April 15, 2025
Evaluation Technical Report	Evaluation Technical Report for HPE Aruba Networking ClearPass Policy Manager 6.11, version 0.2, April 15, 2025
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	HPE Aruba Networking
Developer	HPE Aruba Networking
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD

Item	Identifier
CCEVS Validators	Swapna Katikaneni Marybeth Panock Mike Quintos

3 Architectural Information

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

The Target of Evaluation (TOE) is Aruba ClearPass Policy Manager 6.11.

3.1 TOE Description

The HPE Aruba Networking ClearPass Policy Manager platform provides role- and device-based network access control for employees, contractors and guests across any wired, wireless and VPN infrastructure. ClearPass implements profiling, onboarding, guest access, and health checks facilitating centralized management of network access policies. The network services are the focus of this evaluation and other services are not evaluated.

For the purpose of evaluation, ClearPass is treated as a network infrastructure device offering CAVP tested cryptographic functions, security auditing, secure administration, trusted updates, self-tests, and secure connections to other servers (e.g., to transmit audit records).

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 of this document.

3.3 TOE Architecture

The ClearPass Policy Manager is available either as a hardware or virtual network appliance and is designed to support a wide range of network, wireless and security protocols to support a wide range of clients. However, the evaluation is limited to the hardware network appliances and the secure communication protocols.

There are four TOE appliance models designed to support different numbers of client devices. Each platform differs in CPU performance (e.g., number of cores), available memory, disk performance and storage capacity, and power consumption/supply.

While ClearPass Policy Manager products can be configured as a collection of devices operating in a cluster sharing a common security policy, the TOE configuration subject to this evaluation is limited to a single ClearPass Policy Manager device.

Each ClearPass Policy Manager device is a rack-mountable appliance with Intel Atom, Intel Xeon, or AMD EPYC CPUs running a version of RHEL 8 to host the applications designed to provide the network access control capabilities summarized above. ClearPass includes a version of Hewlett Packard Enterprise OpenSSL Cryptographic Module on Red Hat Enterprise Linux that is used to perform cryptographic functions. This module supports the implementations of IPsec using StrongSwan, TLS/HTTPS using Apache, and SSH using OpenSSH used to secure the communication channels. Remote administration can be performed over TLS/HTTPS or SSH. Exporting audit events and syncing with an NTP server can be performed over IPsec.

3.4 Physical Boundaries

The physical boundaries of the TOE consist of ClearPass Policy Manager device running software version 6.11.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Identification and authentication
4. Security management
5. Protection of the TSF
6. TOE access
7. Trusted path/channels

4.1 Security audit

The TOE is designed to be able to generate logs for a wide range of security relevant events. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to a designated syslog server.

4.2 Cryptographic support

The TOE includes a version of Hewlett Packard Enterprise OpenSSL Cryptographic Module on Red Hat Enterprise Linux that provides key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher-level cryptographic protocols including IPsec, SSH, and TLS/HTTPS.

4.3 Identification and authentication

The TOE offers no TSF-mediated functions except display of a login banner until the administrator is identified and authenticated. The TOE authenticates administrative users accessing the TOE via the command-line interface (local serial console or SSH) or web interface (Web UI) in the same manner using its own password-based authentication mechanism. The TOE also supports public-key based authentication of users through the SSH-based CLI interface and supports certificate authentication for the Web UI.

The TOE supports certificate authentication for TLS and IPsec and supports pre-shared key authentication for IPsec connections. The TOE uses X.509v3 certificates and validates received authentication certificates. OCSP is supported for X509v3 certificate validation.

4.4 Security management

The TOE provides Command Line (CLI) commands (locally via a serial console or remotely via SSH) and a Web-based Graphical User Interface (Web GUI) to access the available functions to manage the TOE security functions. Security management commands are limited to authorized users (i.e., administrators) only after they have been correctly identified and authenticated. The security management functions are controlled through the use of Admin Privileges that can be assigned to TOE users.

4.5 Protection of the TSF

The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

It protects particularly sensitive data such as stored passwords and private cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for audit records).

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

4.6 TOE access

The TOE can be configured to display an informative banner when an administrator establishes an interactive session and subsequently will enforce an administrator-defined inactivity timeout value after which the inactive session (local or remote) will be terminated.

4.7 Trusted path/channels

The TOE protects interactive communication with administrators using a console and SSHv2 for CLI access and TLS/HTTPS for Web UI access. In each case, both the integrity and disclosure protection are ensured via the secure protocol. If the negotiation of a secure session fails or if the user cannot be authenticated for remote administration, the attempted session will not be established.

The TOE protects communication with network peers, such as a syslog server or NTP server, using IPsec connections to prevent unintended disclosure or modification of traffic over the trusted channel.

5 Assumptions & Clarification of Scope

Assumptions

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

- collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 (NDcPP30e)
- Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021 (SSH10)

That information has not been reproduced here and the NDcPP30e/SSH10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP30e/SSH10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the collaborative Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Network Device models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP30e/SSH10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Common Criteria Configuration Guidance HPE Aruba Networking Clearpass Policy Manager 6.11, Version 6.1, April 2025
- ClearPass Policy Manager 6.11.x User Guide, Version 1, March 2025

Any additional customer documentation provided with the product, or available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for HPE Aruba Networking ClearPass Policy Manager 6.11, Version 0.2, April 15, 2025 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP30e/SSH10 including the tests associated with optional requirements. A list of the tested devices is provided in Section 1.1.1 of the AAR, and a diagram of the test environment with a list of test tools is provided in Section 3.4.

8 Evaluated Configuration

The evaluated configuration consists of the following models:

Appliance Model	CPU
N1000	Intel Atom C3758R (Denverton)
N3000	AMD EPYC 9004 Series EPYC 9124 (Zen 4 (Genoa))
N3001	AMD EPYC 9004 Series EPYC 9124 (Zen 4 (Genoa))
Cx000V	ESXi 7.0 on Intel Xeon E-2254ML (Coffee Lake)

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Aruba ClearPass Policy Manager 6.11 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP30e/SSH10.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the HPE Aruba Networking ClearPass Policy Manager 6.11 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP30e/SSH10 related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP30e/SSH10 and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities performed on April 15, 2025, and a summary is included in Section 3.5 of the AAR. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) with the following search terms: "Aruba", "HPE Aruba", "Clearpass", "N1000", "N3000", "N3001", "Cx000V", "CLABV", "C1000V", "C2000V", "C3000V", "Atom C3758R ", "EPYC 9124", "Xeon E-2254ML", "ESXi 7.0", "StrongSwan", "Apache", "OpenSSH", and "OpenSSL".

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the guidance documents listed in Section 6 of this report. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product were not assessed as part of this evaluation. No other versions of the TOE, either earlier or later, were evaluated.

Additional functionality provided by other devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. Note that the collection of devices operating in a cluster is not evaluated as these are most likely the commonly used configurations.

All other items and scope issues have been sufficiently addressed in other sections of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *HPE Aruba Networking ClearPass Policy Manager 6.11 Security Target, Version 1.0, April 15, 2025*.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 3.0e, December 6, 2023 (NDcPP30e).

[5] Functional Package for Secure Shell (SSH), Version 1.0, May 13 2021 (SSH10).

[6] HPE Aruba Networking ClearPass Policy Manager 6.11 Security Target, Version 1.0, April 15, 2025 (ST).

[7] Assurance Activity Report for HPE Aruba Networking ClearPass Policy Manager 6.11, Version 0.2, April 15, 2025 (AAR).

[8] Detailed Test Report for HPE Aruba Networking ClearPass Policy Manager 6.11, Version 0.2, April 15, 2025 (DTR).

[9] Evaluation Technical Report for HPE Aruba Networking ClearPass Policy Manager 6.11, Version 0.2, April 15, 2025 (ETR).