National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Architecture Technology Corporation Machete Router

Report Number: CCEVS-VR-VID11414-2024
Dated: February 15, 2024
Version: 0.2

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

James J Donndelinger
Marybeth Panock
Deron Graves
Fernando Guzman

The Aerospace Corporation

Common Criteria Testing Laboratory

Allison Keenan
Douglas Kalmus
Yoel Fortaleza

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 Architecture Technology Corporation Machete Router solution provided by Architecture Technology Corporation. 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 February 2024. 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 PP-Configuration for Network Devices and Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 which includes the Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12).

The Target of Evaluation (TOE) is the Architecture Technology Corporation Machete Router.

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 Architecture Technology Corporation Machete Router Security Target, version 0.6, November 29, 2023 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	Architecture Technology Corporation Machete Router (Specific models identified in Section 8)

Protection Profile	• PP-Configuration for Network Devices and Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (CFG_NDcPP-VPNGW_V1.2) which includes the following components:
	  ○ Base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e)
	  ○ PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12)

ST	Architecture Technology Corporation Machete Router Security Target, version 0.6, November 29, 2023
Evaluation Technical Report	Evaluation Technical Report for Architecture Technology Corporation Machete Router , version 0.2, January 30, 2024
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	Architecture Technology Corporation
Developer	Architecture Technology Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	James J Donndelinger, Marybeth Panock, Deron Graves, Fernando Guzman

3 Architectural Information

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

The Architecture Technology Corporation Machete Router is a ruggedized, compact, secure and high-performance router that also provides VPN gateway functionality.

3.1 TOE Description

The functions of Machete are implemented in a software suite called ATCorp Routing and Encryption Suite (ARES).

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 Physical Boundaries

Each TOE appliance runs version 2.0 of the ARES software and has physical network connections to its environment to facilitate managing and filtering network traffic. The TOE appliance can also be the destination of network traffic, where it provides interfaces for its own management.

The TSF requires the following equipment/services to be present in the operational environment:

- IPsec Peers
- CRL server
- Syslog server reachable through either an SSH client connection or through a VPN connection
- NTP server reachable through a VPN connection
- Administrative SSH client
- Web Browser for ESXi Console Management

4 Security Policy

This section summaries the security functionality of the TOE:

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

4.1 Security audit

The TOE is capable of auditing all required events and information. Each audit record includes the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.

The TOE protects storage of audit information from modification or deletion. The TOE can transmit audit records to a remote syslog server using either SSH or IPsec.

4.2 Cryptographic support

The TOE contains CAVP-tested cryptographic support 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 and SSH.

4.3 Identification and authentication

The TOE supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length of 6 to 100 characters.

The TOE requires all administrative users to authenticate before allowing the user to perform any actions other than:

- Viewing the warning banner.

After an administrator-specified number of failed attempts, the user account is locked out. The TOE also protects, stores and allows authorized administrators to load X.509.v3 certificates for use to support authentication for IPsec connections.

4.4 Security management

The TOE provides a custom CLI that allows users with the Security Administrator role to administer the TOE locally and remotely. This interface allows the Security Administrator to initiate manual updates, manage cryptographic keys, manage the TOE configuration, and configure audit data transmission.

4.5 Packet filtering

The TOE provides extensive packet filtering capabilities for IPv4, IPv6, TCP, and UDP. The authorized administrator can define packet filtering rules that apply to most every field within the identified packet types. The authorized administrator can define each rule to permit, deny, and log each decision.

4.6 Protection of the TSF

The TOE prevents the reading of secret keys, private keys, and passwords.

The TOE maintains a local real-time clock to provide accurate timestamps. This clock can be periodically updated by synchronizing with an NTP server and/or manually set by a Security Administrator.

The TOE performs a suite of power-up self-tests that verify the correct operation of the entropy source, RAM, and cryptographic algorithms as well as the integrity of the firmware.

The TOE verifies the authenticity and integrity of all firmware updates using ECDSA signature verification. The TOE shuts down if any of these tests fail.

4.7 TOE access

Before establishing an administrative session, the TOE displays an administrator configurable warning banner. The TOE locks inactive local administrative sessions and terminates inactive remote administrative sessions.

The TOE allows the administrator to configure restrictions on the establishment of client IPsec tunnels based on the client IP address, time of day, date, day of week, or day of month. The TOE assigns a private IP address (internal to the trusted network for which the TOE is the headend) to a VPN client upon successful establishment of a session.

4.8 Trusted path/channels

The TOE supports either SSH or IPsec to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. The TOE uses SSH or IPsec to provide the trusted path with remote administrative users as well.

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 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12)

That information has not been reproduced here and the NDcPP22e/VPNGW12 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 NDcPP22e/VPNGW12 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 with the VPNGW PP-Module 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 VPNGW models was not included in the scope of the evaluation and therefore should not to 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 NDcPP22e/VPNGW12 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:

- Machete Router Common Criteria Operational Guidance, Version 1.6, December 14, 2023

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not to 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 Architecture

Technology Corporation Machete Router, Version 0.2, January 30, 2024 (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 NDcPP22e/VPNGW12 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The TOE consists of the following hardware models running ARES v 2.0:

Model Identification	Platform	CPU Architecture	CPU Part Number
MACHETE-FIT2	Fitlet2	Intel Apollo Lake	Atom x7-E3950
MACHETE-OTN4	OnTime 4000 Series	Intel Apollo Lake	Atom x7-E3950
MACHETE-OTN6	OnTime 6000 Series	Intel Apollo Lake	Atom x7-E3950
MACHETE-OTN7	OnTime 7000 Series	Intel Apollo Lake	Atom x7-E3950
MACHETE-DCS2	DCS003289	Intel Apollo Lake	Atom x7-E3950
MACHETE-V1	VMware ESXi v7.0	AMD Ryzen 4000	Ryzen 4600G
MACHETE-AMD-R1	OL-ML100 Series	AMD Ryzen V1000	V1605B
MACHETE-WL1	BKNUC8V5PNB	Intel Whiskey Lake	Core i5-8365U
MACHETE-FIT3	Fitlet3	Intel Elkhart Lake	Atom x6425E

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 Architecture Technology Corporation Machete Router TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/VPNGW12.

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 Architecture Technology Corporation Machete

Router 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 NDcPP22e/VPNGW12 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 NDcPP22e/VPNGW12 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. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Architecture Technology Corporation”, “Machete Router “, “ATCorp”, “ARES”, “OpenSSL”, “Intel Atom x7-E3950”, “AMD Ryzen V1605B”, “Intel Core i5-8365U”, “Intel Atom x6425E”, “Ryzen 4600G”, “TCP”. The search was conducted on January 30, 2024.

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 evaluated configuration instructions in the *Machete Router Common Criteria Operational Guidance, Version 1.6, December 14, 2023*. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that The TOE transmits audit records to the syslog server in real-time. The TOE does not have the ability to cache or retransmit audit records if the syslog server is unavailable.

The TOE allocates 2GB of space to local audit storage. The TOE maintains 4 separate log types and up to 10 files for each log type, one active file and 9 archive files. The current file for each log type is allowed to reach 50MB in size before it is rotated, when the TOE attempts to write an audit log message to an audit file which would increase the size beyond 50MB then that audit log type is rotated. Audit log rotation will delete the oldest archive file, if archiving the current file will create more than 9 archive files. Each archive file is renamed with a suffix .1.gz through .9.gz, indicating the age of the archive file, 1 being the newest and 9 being the oldest. Then the current audit log is compressed and renamed with the suffix .1.gz. Once rotation is completed, a new empty current file is created and the queued audit message is written to the file.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Architecture Technology Corporation Machete Router Security Target, Version 0.6, November 29, 2023*.

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 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for Virtual Private Network (VPN) Gateways, version 1.2, 31 March 2022 (VPNGW12).

[6] Architecture Technology Corporation Machete Router Security Target, Version 0.6, November 29, 2023 (ST).

[7] Assurance Activity Report for Architecture Technology Corporation Machete Router, Version 0.2, January 30, 2024 (AAR).

[8] Detailed Test Report for Architecture Technology Corporation Machete Router, Version 0.2, January 30, 2024 (DTR).

[9] Evaluation Technical Report for Architecture Technology Corporation Machete Router, Version 0.2, January 30, 2024 (ETR)