National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Infinera Corporation mTera Universal Transport Platform version MT5.1.2

Report Number: CCEVS-VR-11153-2021
Dated: August 31, 2021
Version: 0.3

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

Sheldon Durrant
Randy Heimann
Linda Morrison
Clare Parran
The MITRE Corporation

Common Criteria Testing Laboratory

Tammy Compton
Kevin Cummins
Khai Van
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 Infinera mTera Universal Transport Platform solution provided by Infinera 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 August 2021. 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 2.1, 24 September 2018.

The Target of Evaluation (TOE) is the Infinera mTera Universal Transport Platform MT5.1.2.

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 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 mTera Universal Transport Platform version MT5.1.2 Security Target, version 0.5, August 26, 2021 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	Infinera mTera Universal Transport Platform MT5.1.2 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, version 2.1, 24 September 2018
ST	mTera Universal Transport Platform version MT5.1.2 Security Target, version 0.5, August 26, 2021
Evaluation Technical Report	Evaluation Technical Report for Infinera mTera Universal Transport Platform MT5.1.2, version 0.3, August 26, 2021
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	Infinera Corporation
Developer	Infinera Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Sheldon Durrant, Randy Heimann, Linda Morrison, Clare Parran *(The MITRE Corporation)*

3 Architectural Information

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

The Infinera mTera Universal Transport Platform is an extremely flexible and highly efficient transport solution supporting up to 12Tb/s of switching and grooming for OTN, Packet and SONET/SDH leveraging protocol agnostic fabrics and interface cards that can be software configured for OTN, MPLS-TP or Carrier Ethernet on each interface or virtual interface. The Infinera mTera is offered in either a 16-slot chassis or 8-slot chassis.

The mTera is an optical network appliance delivering Wavelength, High-capacity Electrical OTN, and Packet network switching. The mTera supports electrical switching using an agnostic switch fabric. Signals switched by the electrical switch fabric include high-capacity ITU Optical Transport Network (OTN) ODU switching, ITU/ANSI SDH/SONET switching and service oriented MPLS-TP/Ethernet packet switching. The security functions provided include Identification, Authentication, Access Control, Protection of TSF, Confidentiality, Integrity and Auditing.

3.1 TOE Evaluated Configuration

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

3.2 TOE Architecture

The Infinera mTera is a network appliance composed of various module slots. The mTera supports up to two STPM (shelf timing and processor module) cards for management in addition to optical network switch blades. The mTera TOE's management capabilities rely on TL1 commands. The mTera’s interfaces provide TLS and IPsec functionality as well as SSHv2 for management.

The mTera STPM includes an LCI (local craft interface) port for local CLI access and DCN (data communications network) ports for network communications. Though an administrator uses SSH to connect to the mTera through both interfaces, the LCI port does not provide network routing, thus requiring an administrator to connect directly to the LCI port for local console access.

The mTera TOE contains an OpenSSL FIPS object module and a kernel crypto module for cryptographic services. The Kernel Crypto module is used for IPSEC data path (encrypt/decrypt, message authentication, hash) while the OpenSSL module is used for IPSEC Key management (i.e. IKE), SSH and TLS operations. The OpenSSL module is used for secret negotiation, authentication, encrypt/decrypt, message authentication, hashes and DRBG.

3.3 Physical Boundaries

The TOE's physical boundary includes the entire chassis, which contains the STPM management and optical network line cards. The TOE runs firmware version FP.5.1.2p1.

The TOE operates with the following components in the Operating Environment:

- Audit Server – The TOE utilizes an external syslog server to store audit records.
- Authentication Server – The TOE has the ability to use RADIUS servers to authenticate users.
- Time Server – The TOE uses a Network Time Protocol (NTP) server to synchronize its system clock with a central time source.
- SSH Client – The remote administrator uses an SSH client to access the CLI.

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. 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 including start-up and shutdown of the TOE, all administrator actions, and all events identified in the Security Target, Table 2 Auditable 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 in the operational environment.

4.2 Cryptographic support

The TOE includes cryptographic modules that provide 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.

4.3 Identification and authentication

The TOE requires administrators to be identified and authenticated before they can access any TOE security functions. The TOE supports role-based authentication, so user accounts are assigned predefined roles which restrict them based on their assigned role. The TOE maintains these administrator and user attributes which can be defined locally with user names and passwords or can be defined in the context of local RADIUS services. Authentication can be either locally or remotely through an external authentication server, or internally. After an administrator-specified number of failed attempts, the user account is locked out. The TOE's password mechanism provides configuration for a minimum

password length. The TOE also protects, stores and allows authorized administrators to load X.509.v3 certificates for use to support authentication for IPsec, TLS and SSH connections.

4.4 Security management

The TOE provides the administrator role the capability to configure and manage all TOE security functions including cryptographic operations, user accounts, passwords, advisory banner, session inactivity and TOE updates. The management functions are restricted to the administrator role. The role must have the appropriate access privileges or access will be denied. The TOE's cryptographic functions ensure that only secure values are accepted for security attributes.

4.5 Protection of the TSF

The TOE has its own internal hardware clock that provides reliable time stamps used for auditing. The TOE stores passwords on flash and encrypts the passwords using an AES-256-CBC key. The TOE does not provide any interfaces that allow passwords or keys to be read. The TOE also provides integrity and security protection for all communication between its components. This prevents unauthorized modification or disclosure of TSF data during transmission.

The TOE runs self-tests during power up and periodically during operation to ensure the correct operation of the cryptographic functions and TSF hardware. There is an option for the administrator to verify the integrity of stored TSF executable code. The TOE executes self-tests for both the Kernel Crypto module and OpenSSL FIPS Object module.

The TOE includes mechanisms so that the administrator can determine the TOE version and update the TOE securely using digital signatures.

4.6 TOE access

The TOE allows administrators to configure a period of inactivity for administrator and user sessions. Once that time period has been reached while the session has no activity, the session is terminated. All users may also terminate their own sessions at any time. A warning banner is displayed at the management interfaces (local CLI and SSH) to advise users on appropriate use and penalty for misuse of system.

4.7 Trusted path/channels

The TOE uses IPsec to provide an encrypted channel between itself and third-party trusted IT entities in the operating environment including external syslog server, external authentication server and NTP server. The TOE also uses IPsec to encrypt communications between the TOE and external IT entities. The TOE uses TLS to secure network communications with an external optical network peer.

The TOE secures remote communication with administrators by implementing SSHv2 for CLI access. 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.

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 2.1, 24 September 2018

That information has not been reproduced here and the NDcPP21 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 NDcPP21 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.
- 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 NDcPP21 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:

- mTera Universal Transport Platform version MT5.1.2 Security Target, v0.5, August 26, 2021

- Coriant Product Hardening Guide, Version BP11, August 23, 2021
- TL1 Specification, version CP11, August 26, 2021

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 Assurance Activity Report (NDcPP21) for Infinera mTera Universal Transport Platform MT5.1.2, Version 0.3, August 26, 2021 (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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the following series and models:

Product Model	Part Number(s)	CPU
Infinera Corporation mTera Universal Transport Platform – 8 slot chassis	81.71S-MTERA8-R6	See the 8-slot STPM CPU below
Infinera Corporation mTera Universal Transport Platform – 16 slot chassis	81.71S-MTERA-R6	See the 16-slot STPM CPU below
8-slot STPM	82.71C-M8STPM-R6	NXP QorIQ P-4080
16-slot STPM	82.71C-MSTPM-R6	NXP QorIQ P-4080

The STPM cards are management cards that run the software image for the mTera. The only difference between the two STPMs is that they are built with different form factors.

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 mTera Universal

Transport Platform TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP21.

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 Infinera mTera Universal Transport Platform MT5.1.2 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 NDcPP21 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 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 NDcPP21 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/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)
- Exploit / Vulnerability Search Engin (http://www.exploitsearch.net)
- SecurITeam Exploit Search (http://www.securiteam.com)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

on 08/11/2021 with the following search terms:

"Infinera",	"ssh",	"tcp",
"Coriant mTera",	"ike",	"NXP QorIQ P-4080".
"TL1",	"ipsec",	
"radius",	"tls",	

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.

9.1 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 document "Coriant Product Hardening Guide, Version BP11", dated 23 August 2021. No versions of the TOE and software, either earlier or later were evaluated.

Please note that 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, such as a management workstation, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluation and testing of security functional requirements are scoped by the guidance included by the Assurance Activity associated with the Protection Profile claimed by the TOE. There is an inherent risk that elements of the TOE security functionality were not fully evaluated. It is recommended that the TOE be subject to integration testing within its intended environment to ensure proper configuration, compliance, and operation.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *mTera Universal Transport Platform version MT5.1.2 (NDcPP21) Security Target, Version 0.5, August 26, 2021*.

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, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, September 2102.

[4] collaborative Protection Profile for Network Devices, version 2.1, 24 September 2018.

[5] mTera Universal Transport Platform version MT5.1.2 (NDcPP21) Security Target, Version 0.5, August 26, 2021 (ST).

[6] Assurance Activity Report for Infinera mTera Universal Transport Platform MT5.1.2, Version 0.3, August 26, 2021 (AAR).

[7] Detailed Test Report for Infinera mTera Universal Transport Platform MT5.1.2, Version 0.3, August 26, 2021 (DTR).

[8] Evaluation Technical Report for Infinera mTera Universal Transport Platform, Version 0.3, August 26, 2021 (ETR)