National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10

Report Number: CCEVS-VR-VID11502-2025
Dated: 01/16/2025
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

Daniel Fagin
Patrick Mallett, Ph.D.
The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Cummins
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 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 Catonsville, MD, United States of America, and was completed in January 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 2.2e, 23 March 2020 (NDcPP22e).

The Target of Evaluation (TOE) is the Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10.

The 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 Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 Security Target, Version 1.1, 01/15/2025 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	Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e)
ST	Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 Security Target, Version 1.1, 01/15/2025
Evaluation Technical Report	Evaluation Technical Report for Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10, Version 0.3, 01/15/2025
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	Infinera Corporation
Developer	Infinera Corporation
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Daniel Fagin, Patrick Mallett

3 Architectural Information

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

The Target of Evaluation (TOE) is Infinera GX G42 Optical Network Platform running Converged OS (COS) version 6.2.10. The GX G42 is an optical network platform delivering Wavelength, High-capacity Electrical OTN, and Packet network device. This next-generation compact modular transport optical network platform is deployed as part of a point-to-point, point-to-multipoint, or in conjunction with a FlexILS™ network for terrestrial and/or subsea applications. The GX G42 consists of one G42 chassis and provides multi-service client access (e.g., Ethernet, Optical Transport Network (OTN), etc.) to the Dense Wavelength Division Multiplexing (DWDM) transport bandwidth.

The GX G42 provides various security features and protocols including RADIUS, TACACS+, SSHv2, NTP authentication, IPsec (IKEv2), RESTCONF, NETCONF, HTTPS and TLSv1.2.

3.1 TOE Evaluated Configuration

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

3.2 TOE Architecture

The TOE is comprised of both software and hardware. The hardware is comprised of the GX G42 chassis. The software is comprised of the Converged OS (COS) version 6.2.10.

The Infinera GX G42 is a 3 RU chassis that accommodates the pluggable modules identified in the table below:

Hardware Model	Specifications
GX G42 3 RU chassis; includes 1 GX-FAN-CTRL, 2 GX-FAN-XMM4s, and 5 GX-FANMODULE-Ds: -Power Entry Module (PEM) -G42 FIPS Input/Output (I/O) Module -Fan Controller Card (FCC) Module -Fan Modules (XMM4 and sled fan) -G42 Management Control Module (XMM4) -Coherent Module ICE6 (CHM6) Transponder Module -Blank Circuit Packs -Tributary Optical Module (TOM); 400G and 100G variants (a field-replaceable, pluggable module that converts the client optical signals to and from a serial electrical signal)[1]	**Software:** Converged OS (COS) version 6.2.10 **Multi-Processor System:** XMM4 - Intel Atom C3558 (Denverton) CHM6 – NXPLS1012ASE7KKB (ARM Cortex A53) **ASIC**: Atlantic ASIC **Power Supply:** Power Entry Modules (PEMs)—reside in the PEM module slots (labeled as PEM 1, PEM 2, PEM 3, and PEM 4) located at the rear of the chassis (in the upper 1 RU section); up to four AC or four DC PEMs are installed to provide 12V DC power supply throughout the GX G42 **Interfaces:** 10Gbps data communication network (DCN) Ethernet RJ-

[1] Optical network communication is not in the scope of this evaluation

Hardware Model	Specifications
	45 interface. Supports 100M, 1G, and 10G Ethernet port speeds and provides a port for debug and remote management. One 10Gbps auxiliary (AUX) Ethernet interface. Supports 100M, 1G, and 10G port speeds. Two 10Gbps nodal control and timing (NCT) Ethernet interfaces supporting 100M, 1G and 10G port speeds (used for multiple chassis and thus not supported or tested in the evaluated configuration) One 1000Mbps auxiliary Ethernet interface supporting 10M, 100M and 1G port speeds. One 1000MBps craft Ethernet interface supporting 10M, 100M and 1G port speeds One console RS-232 serial port interface One Universal Serial Bus (USB) port interface[2]

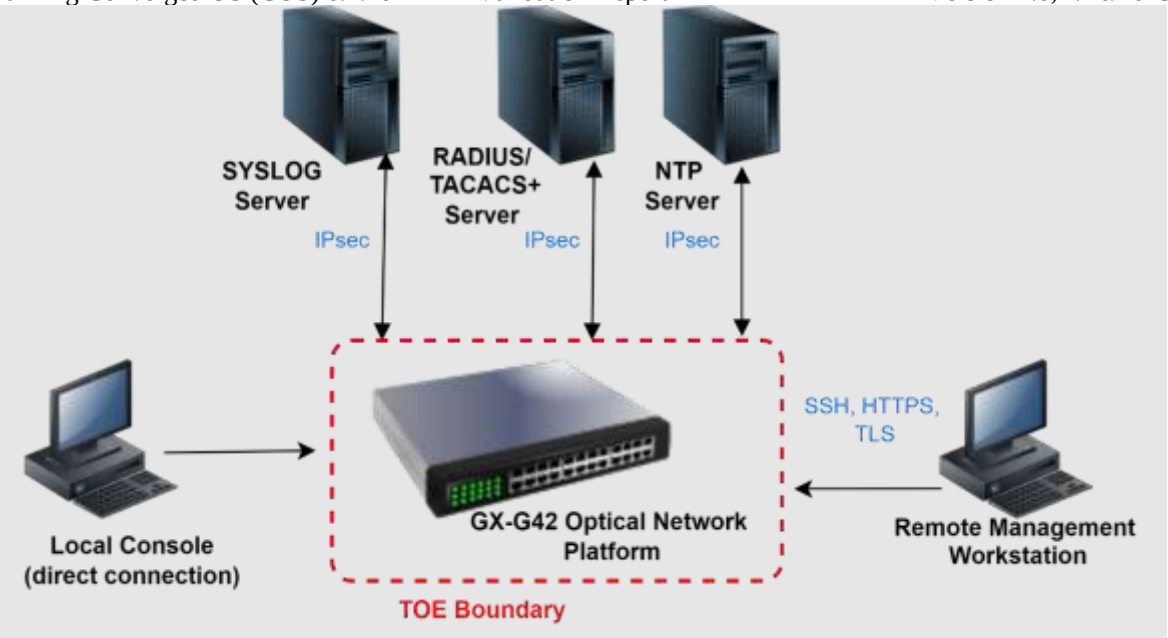
.

3.3 Physical Boundaries

The TOE is a single configuration whose physical boundary includes the entire chassis as identified in the table above. The TOE runs Converged OS (COS) software version 6.2.10.

Error! Reference source not found. Error! Reference source not found. depicts a typical TOE deployment with a single instance of the TOE.

[2] USB ports are disabled in FIPS mode



Error! Reference source not found. TOE Deployment

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

- Syslog (audit) Server – The TOE utilizes an external syslog server over a secure IPsec connection to store audit records.
- RADIUS (authentication) Server – The TOE has the ability to use RADIUS servers over a secure IPsec connection to authenticate users.
- TACACS+ (authentication) Server – The TOE has the ability to use TACACS+ servers over a secure IPsec connection to authenticate users.
- NTP (time) Server – The TOE uses a Network Time Protocol (NTP) server over a secure IPsec connection to synchronize its system clock with a central time source.
- Remote Management Workstation
  - SSH Client – The remote administrator uses an SSH client to securely access the CLI and the NETCONF API.
  - Web browser – The remote administrator uses a web browser with HTTPS/TLS to access the Web UI and the RESTCONF API.
- Local Console – The local administrator uses a direct physical connection to the TOE device.

4 Security Policy

This section summaries the security functionality of the TOE: Security audit

1. Cryptographic support
2. Identification and authentication
3. Security management
4. Packet filtering

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 Table 5 Auditable Events in the Security Target. The TOE stores audit logs locally so they can be accessed by an administrator and is also configured 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 and certificate 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, HTTPS and TLS.

4.3 Identification and authentication

The TOE requires all administrators to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for acknowledging the pre-login warning banner. Authentication can be either locally or remotely through an external RADIUS or TACACS+ authentication server. After an administrator-specified number of failed attempts, the user account is locked out for an administrator specified period of time. 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/IKE and TLS connections.

4.4 Security management

The TOE provides the Security 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 Security Administrator role in accordance with FMT_SMR.2 (see Section 5.1.4.5). The TOE's Security Administrator role is further defined in Section 6.4.5. The role must have the appropriate access privileges or access will be denied.

4.5 Protection of the TSF

The TOE provides reliable time stamps using its own internal hardware clock or by synchronizing with an NTP server over a secure IPsec connection. The TOE stores passwords hashed in the database using PBKDF hmac-sha512. The TOE does not provide any interfaces that allow passwords or keys to be read.

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 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 local and remote administrator 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. An administrator configured login banner is displayed at the management interfaces, local serial console (CLI), SSH CLI and Web UI (HTTPS/TLS), as an advisory and consent warning message regarding use of the TOE.

4.7 Trusted path/channels

The TOE uses IPsec to provide an encrypted channel between itself and the following third-party trusted IT entities in the operating environment: external syslog server, external authentication servers (RADIUS, TACACS+) and NTP server.

The TOE secures remote communication with administrators by implementing SSHv2 (CLI, NETCONF) and HTTPS/TLSv1.2 (Web UI, RESTCONF). 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

5.1 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)

That information has not been reproduced here and the NDcPP22e 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 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.

5.2 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 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 NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

Although the GX G42 performs many networking and cryptographic functions, this evaluation only addresses the functions and cryptographic libraries that provide for the security of the TOE itself as summarized in Section 1.4.1.2 and further specified in Section 5 and 6 of this Security Target. These security functions are drawn from the collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

The following functions are outside the scope of this evaluation and were not tested:

- Multi-chassis management
- Optical network communication
- USB ports (disabled in FIPS mode)
- IPv6
- Dial-out server

The following cryptographic libraries are excluded and have not been subject to evaluation. The functions they provide are outside the scope of this evaluation.

- The CHM6 module's OpenSSL library
- The CHM6 module's implementation of mbedTLS
- The ASIC Atlantic's hardware implementation of AES-GCM-256

6 Documentation

The following documents were available with the TOE for evaluation:

- Infinera GX-G42 Optical Network Platform Release 6.2.10 Hardening Guide, Revision V002, January 2025
- Infinera GX-G42 CLI Security Command Reference Guide, Release 6.2.10, Revision 001, January 2025.

Only the Administrator Guides listed above and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

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 for Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10, Version 0.3, 01/15/2025 (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 NDcPP22e including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in the AAR Section 3.4.

8 Evaluated Configuration

The TOE is comprised of both software and hardware when configured in accordance with the documentation specified in Section 6. The hardware is comprised of the GX G42 chassis. The software is comprised of the Converged OS (COS) version 6.2.10.

The Infinera GX G42 is a 3 RU chassis that accommodates the pluggable modules identified in the table below:

Hardware Model	Specifications
GX G42 3 RU chassis; includes 1 GX-FAN-CTRL, 2 GX-FAN-XMM4s, and 5 GX-FANMODULE-Ds: -Power Entry Module (PEM) -G42 FIPS Input/Output (I/O) Module -Fan Controller Card (FCC) Module -Fan Modules (XMM4 and sled fan) -G42 Management Control Module (XMM4) -Coherent Module ICE6 (CHM6) Transponder	**Software:** Converged OS (COS) version 6.2.10 **Multi-Processor System:** XMM4 - Intel Atom C3558 (Denverton) CHM6 – NXPLS1012ASE7KKB (ARM Cortex A53) **ASIC**: Atlantic ASIC

Hardware Model	Specifications
Module -Blank Circuit Packs -Tributary Optical Module (TOM); 400G and 100G variants (a field-replaceable, pluggable module that converts the client optical signals to and from a serial electrical signal)[3]	**Power Supply:** Power Entry Modules (PEMs)—reside in the PEM module slots (labeled as PEM 1, PEM 2, PEM 3, and PEM 4) located at the rear of the chassis (in the upper 1 RU section); up to four AC or four DC PEMs are installed to provide 12V DC power supply throughout the GX G42 **Interfaces:** 10Gbps data communication network (DCN) Ethernet RJ-45 interface. Supports 100M, 1G, and 10G Ethernet port speeds and provides a port for debug and remote management. One 10Gbps auxiliary (AUX) Ethernet interface. Supports 100M, 1G, and 10G port speeds. Two 10Gbps nodal control and timing (NCT) Ethernet interfaces supporting 100M, 1G and 10G port speeds (used for multiple chassis and thus not supported or tested in the evaluated configuration) One 1000Mbps auxiliary Ethernet interface supporting 10M, 100M and 1G port speeds. One 1000MBps craft Ethernet interface supporting 10M, 100M and 1G port speeds One console RS-232 serial port interface One Universal Serial Bus (USB) port interface[4]

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 Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

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 GX G42 Optical Network Platform

[3] Optical network communication is not in the scope of this evaluation
[4] USB ports are disabled in FIPS mode

running Converged OS (COS) 6.2.10 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 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)

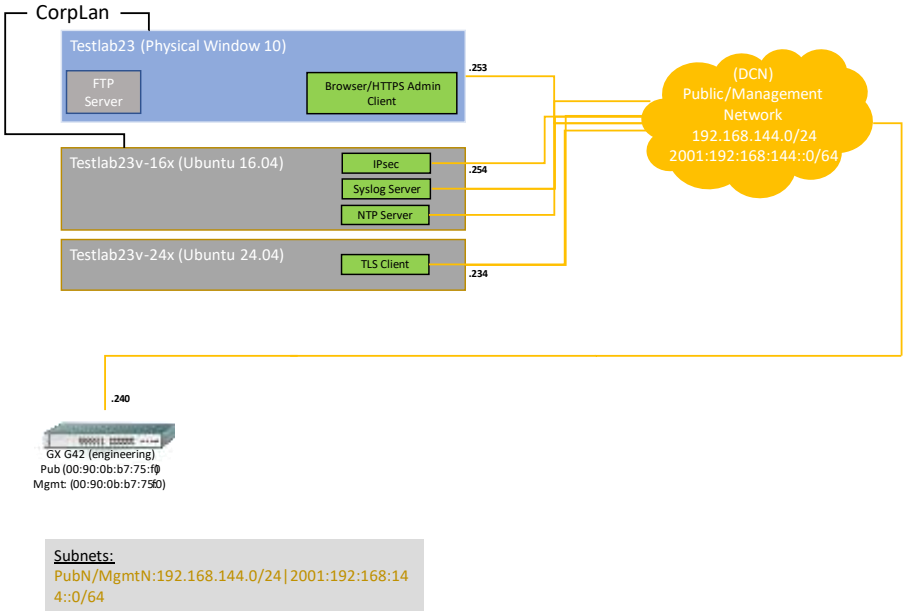
The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

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 and recorded the results in a Test Report, summarized in the AAR.

Testing took place from March 2024 through January 2025 within the Gossamer Security Solutions laboratory in Columbia, MD following the procedures identified in the Gossamer Quality Manual with no deviations. Tests were executed by the Gossamer evaluation team. The developer was available to assist during the testing phase.



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 and fuzz testing. None of the public search for vulnerabilities, or the fuzz testing uncovered any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- 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/)

The search was performed on 12/19/2024 with the following search terms: : "Infinera", "GX-G42", "Converged OS", "COS", "Infinite Capacity Engine", "ICE6", "ICE7", "Infinera GX G40 G42 Cryptographic Module", "Intel Atom C3558", "NXP LS1012A", "NXPLS1012A".

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 Administrator Guide documents listed in Section 6. 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 the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 Security Target, Version 1.1, 01/15/2025*

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 2.2e, 23 March 2020 (NDcPP22e).

[5] Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10 Security Target, Version 1.1, 01/15/205 (ST).

[6] Assurance Activity Report for Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10, Version 0.3, 01/15/2025 (AAR).

[7] Detailed Test Report for Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10, Version 0.3, 01/15/2025 (DTR).

[8] Evaluation Technical Report for Infinera GX G42 Optical Network Platform running Converged OS (COS) 6.2.10, Version 0.3, 01/15/2025 (ETR)