National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena 5400 Series Packet Optical Platform

Report Number: CCEVS-VR-VID10678-2016
Version 1.0
February 2, 2016

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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jean Petty, Senior Validator
The MITRE Corporation

Sheldon Durrant, Lead Validator
The MITRE Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
Jeff Barbi
David Cornwell
Herbert Markle
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Ciena 5400 Series Packet Optical Platform provided by Ciena 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in January 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP).

The Target of Evaluation (TOE) is the Ciena 5400 Series Packet Optical Platform, which is a packet-optical switching platform. It is also known as the Ciena 5400 Series. The 5400 Series contains two models: the Ciena 5430 and Ciena 5410. Each of these devices runs Linux kernel version 3.4.36 and provides identical security functionality to one another.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDPP Assurance Activities. 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 *Ciena 5400 Series Packet Optical Platform Security Target v1.0*, dated January 11, 2016 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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	Ciena 5400 Series Packet Optical Platform Models: Ciena 5430 and Ciena 5410
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional SSH requirement) and Errata #3
Security Target	Ciena 5400 Series Packet Optical Platform Security Target v1.0, January 11, 2016
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Ciena 5400 Series Packet Optical Platform" Evaluation Technical Report v1.0 dated February 1, 2016
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Ciena Corporation
Developer	Ciena Corporation
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Jean Petty, The MITRE Corporation Sheldon Durrant, The MITRE Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNDETECTED_ACTIONS** — Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.PROTECTED_COMMUNICATIONS —** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- **O.VERIFIABLE_UPDATES —** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- **O.SYSTEM_MONITORING —** The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- **O.DISPLAY_BANNER —** The TOE will display an advisory warning regarding use of the TOE.

- **O.TOE_ADMINISTRATION —** The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.RESIDUAL_INFORMATION_CLEARING —** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.SESSION_LOCK —** The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.TSF_SELF_TEST —** The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly**.**

3.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional SSH requirement) with Errata #3 to which this evaluation claimed exact compliance.

- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 Section 6 of the Security Target. The switch functionality included in the product and described in Section 1.3 of the Security Target 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.

The Ciena 5400 Series is a family of standalone single hardware appliances that run Linux. The Target of Evaluation (TOE) is the general network device security functions that are provided by the Ciena 5400 Series, such as security auditing, trusted communications, security management, and identification and authentication. The appliances provide command line and TL1 interfaces to the TOE’s security functionality as well as the switching behavior that is beyond the scope of the claimed Protection Profile.

The purchased product contains the following component that is required for installation only. This component is not part of the TSF relevant functionality that is being evaluated as the TOE and is disabled for operations.

- CORBA administrative interface – by default, the CORBA administrative interface that can be used to interact with the TSF does not provide security. In the evaluated configuration, it will be disabled following initial setup so that all remote administrative communications use SSH.

- FTP, HTTP, TELNET, TELNET_TLS, SNMP – these protocols must be locked (disabled) in the evaluated configuration.

Additionally, the TOE includes a number of functions that are outside the scope of the claimed Protection Profile. These functions are not part of the TSF because there are no SFRs that apply to them.

The exclusion of these functionalities do not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

4 Architectural Information

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

The Ciena 5400 Series Packet Optical Platform is a family of hardware devices that provides OSI Layer 2 network traffic management services. It is a packet-optical switching platform that enables users to direct traffic to designated ports, giving them control of network availability for specific services. The system features an agnostic switch fabric that is capable of switching SONET/SDH, OTN, and Ethernet/MPLS networks.
The Ciena 5400 Series supports OC-48/STM-16 and OC-192/STM-64, OTU1/2/3/4, and 1/10/40/100G Ethernet interfaces to provide up to 15 Tbps switching capacity using a combination of:

- Up to 30 line modules on the 5430 chassis
- Up to 10 line modules on the 5410 chassis

The Ciena 5400 Series is a family of standalone single hardware appliances that run Linux. The Target of Evaluation (TOE) is the general network device security functions that are provided by the Ciena 5400 Series, such as security auditing, trusted communications, security management, and identification and authentication. The appliances provide command line and TL1 interfaces to the TOE’s security functionality as well as the switching behavior that is beyond the scope of the claimed Protection Profile.

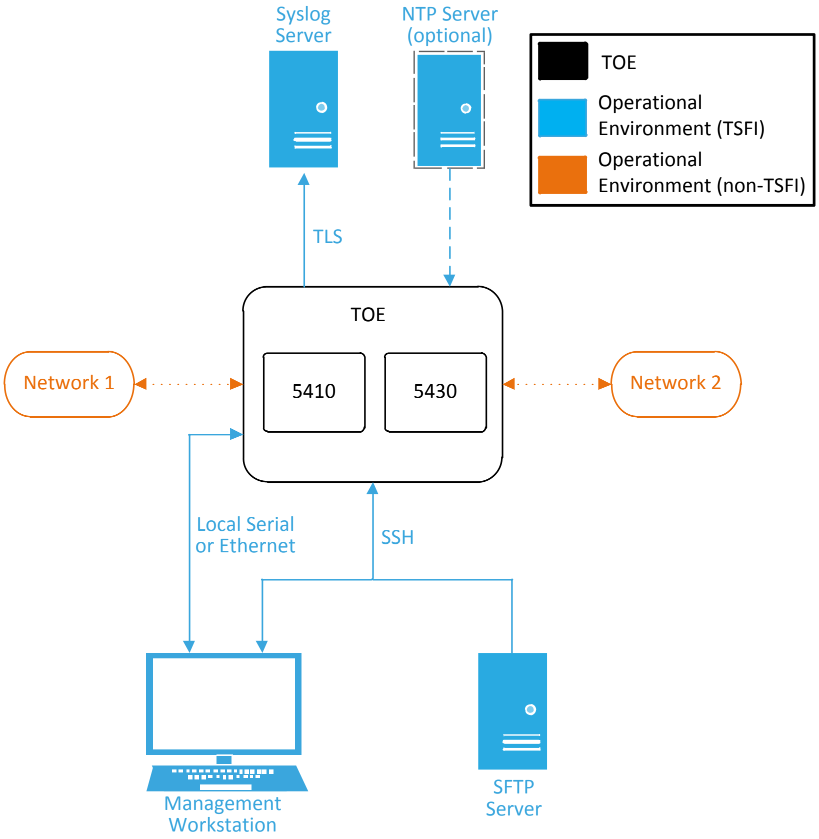

Figure 4-1: TOE Boundary

In practice, the TOE will be deployed to perform OSI Layer 2 switching functions and will be connected to a number of other network traffic infrastructure equipment. This has not been depicted in detail because this capability is out of scope of the TOE from a security functional perspective.

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Usage/Purpose Description for TOE performance
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. The TOE can be managed remotely, in which case the management workstation requires an SSH client, or locally, in which case the management workstation must be physically connected to the TOE using the serial port and must use a terminal emulator that is compatible with serial communications.
NTP Server	A system that provides an authoritative and reliable source of time using network time protocol (NTP).
Syslog Server	A general-purpose computer that is running a syslog server, which is used to store audit data generated by the TOE.
Update Server	A server running the secure file transfer protocol (SFTP) that is used as a location for storing product updates that can be transferred to the TOE.

5 Security Policy

5.1 Security Audit

The TOE provides extensive auditing capabilities. The security log includes detailed records of all user activity including events related to authentication, management, and session termination. Establishment, termination, and failure to establish trusted communications is also audited. The TOE generates audit logs using syslog, and the collected audit data can be transmitted securely to a remote server in the Operational Environment.

The TOE records, for each audited event, the date and time of the event, the type of event, the subject's claimed identity, and the outcome (success or failure) of that event. Depending on the specific type of event, additional data may be included in the audit record.

5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS trusted communications for remote administration, remote storage of audit data, and secure download of TOE updates. Asymmetric keys used by the TSF are generated in accordance with NIST SP 800-56. The TOE uses CAVP-validated cryptographic algorithms (see Table 4 for certificate references).

Table 4 CAVP References

Algorithm	Cert. #
AES	3753
RSA	1930
SHS	3124
HMAC	2456
DRBG	1029

The TOE collects entropy from a third-party hardware source contained within the device to ensure sufficient randomness for secure key generation.

5.3 User Data Protection

The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Any data that terminates before the minimum packet size is reached is padded with zeroes.

5.4 Identification and Authentication

All users must be identified and authenticated to the TOE via locally-defined username and password or username and SSH public key before being allowed to perform any actions on the TOE, except viewing a banner. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum security strength through the set of supported characters and configurable minimum password length. As part of connecting to the TOE locally, using the management workstation, password data will be obfuscated as it is being input.

5.5 Security Management

The product maintains several pre-defined roles for the TL1 administrative interface. Of these, the Account Administrator (AA) is the only administrative role that has the ability to manage the TSF, so it is the only TL1 role that is within the scope of the TOE. The TOE also provides a separate superuser role that is used exclusively for managing the TSF using the MCLI. The superuser and AA roles are analogous to the role of Security Administrator as defined by the NDPP. The remaining roles perform network management related functionality that is not considered to be part of the TSF.

5.6 Protection of the TSF

The TOE is expected to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE stores passwords in an obfuscated format. The cryptographic module prevents the unauthorized disclosure of secret cryptographic data, and administrative passwords are hashed using SHA-256. The TOE maintains system time with either its local hardware clock or optionally with an NTP server synchronization. TOE software updates are acquired using SFTP and initiated using the MCLI. Software updates are digitally signed to ensure their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

5.7 TOE Access

The TOE can terminate inactive sessions after an administrator-configurable time period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a configurable banner on both the MCLI and TL1 interfaces that is displayed prior to use of any other TSF.

5.8 Trusted Path/Channels

The TOE establishes a trusted path to the TOE using SSH for MCLI and TL1 administration. The TOE also establishes trusted channels for sending audit data to a remote syslog server using TLS and for downloading software updates and manually transferring audit records using SFTP (FTP over SSH).

6 Documentation

The vendor provides guidance documentation:

- Ciena 5400 Series Packet Optical Platform Supplemental Administrative Guide v1.0
- Turn-up and Test – 009-3251-002
- Alarm and Trouble Clearing Procedures Manual - 009-3251-003
- Service Manual - 009-3251-004
- Node Manager User Guide - 009-3251-005
- System Description - 009-3251-006
- 5430 Switch Hardware Installation – 009-3251-001
- 5410 Switch Hardware Installation – 009-3251-019
- TL1 Interface Manual – 009-2009-086

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more the Ciena 5400 Series Packet Optical Platform standalone network hardware appliances. Models include:

- Ciena 5410 Packet Optical Platform
- Ciena 5430 Packet Optical Platform

To use the product in the evaluated configuration, the product must be configured as specified in the *Ciena 5400 Series Packet Optical Platform Supplemental Administrative Guide v1.0* (AGD) document.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in the *Evaluation Technical Report for a Target of Evaluation "Ciena 5400 Series Packet Optical Platform" Evaluation Technical Report v1.0 dated February 1, 2016*, which is not publically available.

8.1 Test Configuration

The evaluation team configured each tested model of the TOE according the *Ciena 5400 Series Packet Optical Platform Supplemental Administrative Guide v1.0* (AGD) document for testing.

The evaluation team set up a test environment for the independent functional testing that allowed them to perform the full suite of test assurance activities on the following two models 5410 and 5430. This ensured that the results would be consistent for both models.

The TOE was configured to communicate with the following environment components:

- SFTP Server to acquire updates
- Syslog Server to external audit storage
- NTP Server to acquire the time

The following test tools were installed on a separate workstation (management workstation)

- WireShark: version 1.12.8
- Bitvise SSH Client: version 6.24 and 6.43
- PuTTY: version beta 0.66

*Only the test tools utilized for functional testing have been listed.

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Ciena 5400 models by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test enumerates network port and service information to determine if any ports were open and running services outside of the TOE standard configuration.
- Force SSHv1
  This attack determines if the client will accept both SSHv1 and SSHv2 connections when the TOE claims to only support SSHv2
- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by observing the difference in server response times to valid username login attempts.

The TOE successfully prevented any attempts of subverting its security.

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 4 and CEM version 3.1 rev 4. The evaluation determined the Ciena 5400 Series TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 Ciena 5400 Series product that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Security Requirements for Network Devices Protection Profile (NDPP).

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's TOE Summary Specification as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, 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 NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, 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 evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 addressed the vulnerability analysis Assurance Activities in the NDPP, 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 test activities 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 performed the Assurance Activities in the NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Ciena 5400 Series Packet Optical Platform Supplemental Administrative Guide v1.0* (AGD) document.

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. All other functionality provided by the devices needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product’s evaluation is *Ciena 5400 Series Packet Optical Platform Security Target v1.0* dated January 11, 2016.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CES	Carrier Ethernet Solutions
CLI	Command Line Interface
CSP	Critical Security Parameter
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code
KAS	Key Agreement Scheme
MAC	Media Access Control
NDPP	Network Device Protection Profile
POST	Power On Self-Test
NTP	Network Time Protocol
QoS	Quality of Service
RSA	Rivest Shamir Adelman (encryption algorithm)
SAOS	Service Aware Operating System
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell

14 Terminology

Terminology	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Role	An assigned role gives a user varying access to the management of the TOE.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Ciena 5400 Series Packet Optical Platform Security Target v1.0, dated January 11, 2016
6. Ciena 5400 Series Packet Optical Platform Supplemental Administrative Guide v1.0, dated December 18, 2015