National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena 8700 Packetwave Platform with SAOS 8.5

Report Number: CCEVS-VR-VID10729-2017
Version 1.0
July 14, 2017

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

Patrick Mallett PhD, Lead Validator
The MITRE Corporation

Common Criteria Testing Laboratory

Christopher Gugel, CC Technical Director
David Cornwell
Justin Fisher
Brad Isbell
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Annapolis Junction, 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 8700 Packetwave Platform with SAOS 8.5 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 Annapolis Junction, Maryland, United States of America, and was completed in July 2017. 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 collaborative Protection Profile, version 1.0 (NDcPP).

The Target of Evaluation (TOE) is the Ciena 8700 Packetwave Platform standalone network switch that receives data from an external source and forwards that data to one or many ports. The switch runs the Ciena Service Aware Operating System (SAOS) 8.5, with uniform security functionality between each of the hardware appliance models.

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 NDcPP. 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 NDcPP Evaluation 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 8700 Packetwave Platform with SAOS 8.5 Security Target v1.0*, dated June 8, 2017 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 8700 Packetwave Platform running Ciena Service Aware Operating System (SAOS) 8.5 *Refer to Table 2 for Models and Specifications
Protection Profile	Collaborative Protection Profile for Network Devices, Version 1.0, 27 February 2015, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Ciena 8700 Packetwave Platform with SAOS 8.5 Security Target v1.0, June 8, 2017
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Ciena 8700 Packetwave Platform with SAOS 8.5" Evaluation Technical Report v1.0 dated June 8, 2017
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, Annapolis Junction, Maryland
CCEVS Validators	Jean Petty, The MITRE Corporation Patrick Mallett, 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 the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- 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.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.

3.2 Threats

The following lists the threats addressed by the TOE.

- **T.UNAUTHORIZED_ADMINISTRATOR_ACCESS** – Threat agents may attempt to gain administrator access to the TOE's management functionality through nefarious means such as replay, impersonation, or man-in-the-middle attacks.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak keys or cryptographic algorithms to gain unauthorized access to protected data at rest or in transit.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may exploit unencrypted communications channels to access sensitive data or manipulate data in transit.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols to access a remote endpoint used by the TOE using shared, static, plaintext, or default credentials.
- **T.UPDATE_COMPROMISE –** Threat agents may exploit an unpatched system or provide a malicious update to the TOE in order to cause a known failure.
- **T.UNDETECTED_ACTIVITY** – A malicious administrator may perform improper activities on the TOE and have the ability to prevent audit records of the activity from being generated or to remove all traces of their activities.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** A self-protection mechanism of the TOE may fail or be improperly implemented, allowing a threat agent to access functions or data that were meant to be protected.
- **T.PASSWORD_CRACKING –** A weak administrator password may allow a malicious actor to access administrative functionality through password guessing or brute force exhaustion.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** A component of the TOE responsible for implementing security functionality may fail without administrator awareness.

3.3 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 collaborative Protection Profile for Network Devices, Version 1.1, 27 February 2015, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.
- 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 security functionality 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 ST. The Layer 2 network switching 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 evaluated configuration of the TOE includes the Ciena 8700 Packetwave Platform product that is comprised of one or more of the product models listed in Table 2 and includes version 8.5 of its software. The TOE includes several types of licenses – in the evaluated configuration, the Enhanced Security license is required and all others are non-security-relevant. In the evaluated configuration, the TOE uses SSH to secure remote command-line administration, transfer of log files, and acquisition of software updates, and TLS to secure remote syslog transfer and RADIUS authentication. The TOE provides a FIPS 140-2 conformant mode of operation; the non-FIPS mode is excluded from the evaluation. The TOE includes supplemental administrative guidance in order to instruct Administrators in the secure installation and operation of the TOE. Adherence to this guidance is sufficient to ensure that the TOE is operated in accordance with its evaluated configuration.

The following product capabilities are excluded from the evaluated configuration; administrators enabling and using this functionality are warned that no claim as to the security of the TOE is asserted by the test laboratory when it is not deployed and operated in its evaluated configuration.

- **Non-FIPS mode of operation** - The TOE includes a FIPS compliant mode of operation which allows the TOE to use only approved ciphersuites for SSH communications and to perform cryptographic self-tests on system startup. This mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
- **Remote Telnet interface** - The TOE includes both Telnet and SSH interfaces for administration. Telnet is acceptable to use locally via serial connection, but in the evaluated configuration this remote service will be disabled.
- **DHCP Server interface -** The TOE includes this interface that supports communications between the TOE and a DHCP Server in the Operational Environment; however, it will be disabled in the evaluated configuration.

- **SNMP interface** - The TOE includes this interface which is used to allow the 8700 Series to communicate with RADIUS/TACACS+ servers via SNMP and also listen for SNMP traps from other network devices. In the evaluated configuration, this will be disabled.
- **TACACS+ Interface** - The TOE supports this interface which is used to provide authentication services, but will be disabled in this evaluated configuration.
- **Network Configuration Protocol (NETCONF) –** the installation, deletion, and manipulation of network configuration over SSH will not be included.
- **Diagnostic (Diag) role** - The TOE supports a Diagnostic role; however, this role is only used for non-security-relevant service functionality and will be excluded from the evaluated configuration when the TOE is in an operational state.

The exclusion of these functions does not affect compliance to the collaborative Protection Profile for Network Devices, version 1.0.

4 Architectural Information

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

4.1 TOE Introduction

Ciena Carrier Ethernet Solutions 3900/5100 Series is a hardware appliance whose primary functionality is related to the handling of network traffic. The NDcPP defines a network device as "a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise." Additionally, the NDcPP says that example devices that fit this definition include routers, firewalls, intrusion detection systems, audit servers, and switches that have Layer 2 functionality. The TOE is a packet networking switch that performs second tier aggregation of network traffic that interfaces with an IP/MPLS domain.

The TOE consists of one or more models as specified in Section 4.2 below and includes the software version SAOS 8.5.

4.2 Physical Boundary

The TOE is comprised of both software and hardware. The hardware is comprised of the following:

Table 2 – Hardware Models and Specifications

Platform	4-Slot	10-Slot
Number of line module slots	4	10
Control/timing/switch modules	2, 1+1 redundant	2, 1+1 redundant
Switch modules	1, 1:N redundant	1, 1:N redundant
Equipped capacity	3T	3T
Input/output module (alarms/timing)	1	1
Cooling	One fan unit: six impellers on three axes	One fan unit: ten impellers on five axes
Power units	2	4
Power Options	AC, DC	AC, DC

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.
OCSP Server	The OCSP server is used by the TOE to validate certificate revocation status.
SFTP Server	The SFTP server is used for storage of TOE software/firmware updates that can be retrieved remotely by the TSF. The Administrator can also transfer the security, event, and command logs to another or the same SFTP server over this interface. Communications over this interface are secured using SFTP via SSH where the TOE is acting as an SSH client.
Syslog Server	A remote server that is used to store syslog audit records that the TOE transmits to it. The TOE communicates with the syslog server using TLS.

Component	Usage/Purpose Description for TOE performance
RADIUS Server	The RADIUS server enables user authentication and is secured using TLS. Note that while RADIUS authentication is supported by the TOE, the use of it is not mandatory.

5 Security Policy

5.1 Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. The TOE transmits syslog audit data securely to a remote syslog server using TLS. The TOE also maintains security, event, and command logs internally. The contents of these logs can be configured to be transferred automatically to a remote SFTP server. Each audit record contains the subject information, time stamp, message briefly describing what actions were performed, outcome of the event, and severity. All audit record information is associated with the user of the TOE that caused the event where applicable. Locally-stored audit data can be deleted by a user with the Super role but it is read-only for all other roles. Local audit data is overwritten when the local storage space is full.

5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and TLS trusted communications. Asymmetric keys that are used by the TSF are generated in accordance with FIPS PUB 186-4 and are established in accordance with NIST SP 800-56A and NIST SP 800-56B. The TOE collects entropy from software-based sources contained within the device to ensure sufficient randomness for secure key generation. Cryptographic keys are destroyed when no longer needed. Ciena's cryptographic implementation was validated against CAVP in order to ensure correct functionality of cryptographic behavior. The following table contains the CAVP algorithm certificates.

Table 4 –CAVP References

Algorithm	Cert. #
AES	4470
DRBG	1454
DSA	1198
ECDSA	1092
HMAC	2967
KAS ECC	120
RSA	2445
SHS	3682

5.3 Identification and Authentication

Users authenticate to the TOE either via the local console or remotely using SSH for management of the TSF. All users must be identified and authenticated to the TOE before being allowed to perform any actions on the TOE other than viewing the pre-authentication warning banner. Users can be authenticated using RADIUS by connecting to a RADIUS server in the Operational Environment over TLS. Depending on the configuration of the TSF and the method used to access the TOE, the user can also authenticate using a locally-defined username/password combination (as opposed to credentials being defined in RADIUS) or through SSH public key-based authentication. The TOE provides complexity rules that ensure that user-defined passwords will meet a minimum security strength. As part of connecting to the TOE locally using the management workstation, password data will be obfuscated as it is being input. The TSF connects to an OCSP server to verify certificate revocation status and includes a mechanism internally to

determine the validity of certificates. The TOE also provides support for X.509v3 certificates for authentication.

5.4 Security Management

The TOE maintains distinct roles for user accounts: Limited, Admin, and Super. These roles define the management functions for each user on the TOE. A user who is assigned one of these roles is considered to be an administrator of the TOE, but the functions they are authorized to perform will differ based on the assigned role. The three roles are hierarchical, so each role has all of the privileges of the role(s) below it. A Limited user has read-only privileges for certain TOE functions and data whereas a user with the Admin role has read/write permission over most TOE functionality. The Super role is the highest role and can perform read/write operations on all TOE functions and data, including those functions that the Admin role is not authorized to perform. All administration of the TOE can be performed locally using a management workstation with a terminal client, or remotely using an SSH remote terminal application.

5.5 Protection of the TSF

The TOE is able to ensure the security and integrity of all data that is stored locally and accessed remotely. The TOE provides no interface for the disclosure of secret cryptographic data, and administrative passwords themselves are hashed using SHA-512. The TOE maintains system time locally based on an administratively-defined time. TOE software updates are acquired using SFTP and initiated using the CLI. The TOE software version is administratively verifiable and software updates are signed to provide assurance of their integrity. The TSF validates its own correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

5.6 TOE Access

The TSF 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 displays a configurable warning banner prior to its administrative use.

5.7 Trusted Path/Channels

The TOE establishes a trusted path to the TOE using SSH for remote administration. The TOE establishes trusted channels using TLS for sending syslog audit data to a remote syslog server and SSH for sending stored security, command, and event log data to a remote SFTP server. In addition, the TOE uses the SFTP interface to download updates and store log files. The TOE may also connect to the RADIUS server for user authentication using TLS.

6 Documentation

The vendor provided the following guidance documentation in support of the evaluation:

- Ciena 8700 Packetwave Platform Supplemental Administrative Guidance, Version 1.0
- 8700 SAOS 8.5 Product Fundamentals – 380-1875-010
- 8700 SAOS 8.5 Administration and Security – 380-1875-301
- 8700 SAOS 8.5 Base Configuration – 380-1875-310
- 8700 SAOS 8.5 Software Management and Licensing – 380-1875-221
- 8700 4-slot Installation – 380-1875-201
- 8700 10-slot Installation – 380-1875-202
- 8700 SAOS 8.5 Command Reference – 380-1875-810
- 8700 SAOS 8.5 System Event Reference – 380-1875-840
- 8700 SAOS 8.5 Fault, and Performance Management – 380-1875-500
- 8700 SAOS 8.5 Planning, Engineering, and Ordering Guide – 380-1875-221

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Ciena 8700 standalone network hardware appliances that run SAOS version 8.5.

To use the product in the evaluated configuration, the product must be configured as specified in the *Ciena 8700 Packetwave Platform with SAOS 8.5, Supplemental Administrative Guidance, Version 1.0* 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 proprietary *Evaluation Technical Report for a Target of Evaluation "Ciena 8700 Packetwave Platform with SAOS 8.5" v1.0 dated June 8, 2017,* as summarized in the publicly available *Assurance Activity Report for a Target of Evaluation "Ciena 8700 Packetwave Platform with SAOS 8.5" Assurance Activities Report v1.0 dated June 8, 2017*.

8.1 Test Configuration

The evaluation team configured the TOE according the *Ciena 8700 Packetwave Platform with SAOS 8.5, Supplemental Administrative Guidance, Version 1.0* (AGD) document for testing. Based on the guidance provided in the "Network Device Equivalency Considerations" section of the Evaluation Activities for Network Device cPP Supporting Document, the evaluation laboratory determined that the 4-slot and 10-slot models of the TOE could be reasonably expected to exhibit identical security characteristics and therefore testing was conducted entirely on the 4-slot model.

The evaluation team conducted testing in-person at a Ciena facility in Hanover, Maryland in a physically secured laboratory space and on an isolated network. During the course of this testing, audit log data was reviewed at the start of the day in order to ensure that the TOE was in a known state and had not been modified during the evaluators' absence. Testing was performed against both local and remote management interfaces.

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

- Management workstation for local and remote administration
- Syslog server for recording of syslog data
- SFTP server for recording of log file data and storage of software updates
- LDAP server for environmental authentication
- OCSP responder for certificate status checking

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

- WireShark: version 2.2.2
- Bitvise SSH Client: version 7.24

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

8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the TOE 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 NDcPP 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 and initially discovering no known vulnerabilities, the team 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
- CLI Privilege Escalation
- Fuzzing – Mutated TYPE and CODE
- Fuzzing – Mutated remaining field
- Force SSHv1

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 Evaluation 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 TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Evaluation Activities specified in the NDcPP.

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 8700 product that is consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Evaluation Activities specified in the NDcPP Supporting Documents in order to verify that the specific required content of the TOE Summary Specification is present, consistent, and accurate.

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. Additionally, the evaluator performed the Evaluation Activities specified in the NDcPP Supporting Documents 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 Evaluation Activities specified in the NDcPP Supporting Documents 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 Evaluation Activities in the NDcPP Supporting Documents and recorded the results in a Test Report, summarized in the Evaluation Technical Report and sanitized for non-proprietary consumption in the Assurance Activity 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 NDcPP Supporting Documents, 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 evaluation team also ensured that the specific vulnerabilities defined in the NDcPP Supporting Documents were assessed and that the TOE was resistant to exploit attempts that utilize these vulnerabilities.

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 requirements in the NDcPP Supporting Documents, 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 Evaluation Activities in the NDcPP Supporting Documents, 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 8700 Packetwave Platform with SAOS 8.5, Supplemental Administrative Guidance, Version 1.0* 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 8700 Packetwave Platform with SAOS 8.5 Security Target, Version 1.0* dated June 8, 2017.

13 List of Acronyms

Acronym / Abbreviation	Definition
CC	Common Criteria
CLI	Command-Line Interface
cPP	collaborative Protection Profile
FTP	File Transfer Protocol
IP	Internet Protocol
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
OS	Operating System
PP	Protection Profile
RBG	Random Bit Generator
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSH	Secure Shell

14 Terminology

Term	Definition
Administrator	A user who is assigned any of the three administrative roles defined for the TOE: Limited, Admin, and Super. While these are all considered to be administrators, the assigned role determines the specific level of privilege a given administrator has to interact with TOE functions and data.
Security Administrator	The claimed Protection Profile defines a single Security Administrator role that is authorized to manage the TOE and its data. Since this particular TOE defines three separate administrator roles, an administrator is considered to be the Security Administrator for only the management functions that are associated with their assigned role.
Trusted Channel	An encrypted connection between the TOE and a system in the Operational Environment.
Trusted Path	An encrypted connection between the TOE and the application a Security Administrator uses to manage it (web browser, terminal client, etc.).
User	In a CC context, any individual who has the ability to access the TOE functions or data.

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 8700 Packetwave Platform with SAOS 8.5 Security Target, Version 1.0
6. Ciena 8700 Packetwave Platform with SAOS 8.5 Supplemental Administrative Guidance, Version 1.0