National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena Carrier Ethernet Solutions 3900/5400 Series

Report Number: CCEVS-VR-VID10679-2015
Version 1.0
January 26, 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
Kevin Le
Herbert Markle
Christopher Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 EXECUTIVE SUMMARY 4
2 IDENTIFICATION 5
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 6
4 ARCHITECTURAL INFORMATION 8
TOE INTRODUCTION 8
PHYSICAL BOUNDARIES 8
5 SECURITY POLICY 10
SECURITY AUDIT 10
CRYPTOGRAPHIC SUPPORT 10
USER DATA PROTECTION 10
IDENTIFICATION AND AUTHENTICATION 11
SECURITY MANAGEMENT 11
PROTECTION OF THE TSF 11
TOE ACCESS 11
TRUSTED PATH/CHANNELS 11
6 DOCUMENTATION 12
7 EVALUATED CONFIGURATION 13
8 IT PRODUCT TESTING 14
TEST CONFIGURATION 14
DEVELOPER TESTING 14
EVALUATION TEAM INDEPENDENT TESTING 14
EVALUATION TEAM VULNERABILITY TESTING 15
9 RESULTS OF THE EVALUATION 16
EVALUATION OF THE SECURITY TARGET (ASE) 16
EVALUATION OF THE DEVELOPMENT (ADV) 16
EVALUATION OF THE GUIDANCE DOCUMENTS (AGD) 16
EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC) 17
EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE) 17
VULNERABILITY ASSESSMENT ACTIVITY (VAN) 17
SUMMARY OF EVALUATION RESULTS 17
10 VALIDATOR COMMENTS 18
11 ANNEXES 19
12 SECURITY TARGET 20
13 LIST OF ACRONYMS 21
14 TERMINOLOGY 22
15 BIBLIOGRAPHY 23

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Ciena Carrier Ethernet Solutions (CES) Solutions 3900/5400 Series 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 Carrier Ethernet Solutions 3900/5100 Series 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) 6.14, with uniform security functionality between each of the hardware appliances.

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 Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0*, dated January 7, 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 Carrier Ethernet Solutions 3900/5100 Series running Ciena Service Aware Operating System (SAOS) 6.14 *Refer to Table 2 for Models and Specifications
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional SSH requirement) and Errata #3
Security Target	Ciena Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0, January 7 2016
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Ciena Carrier Ethernet Solutions 3900/5100 Series" Evaluation Technical Report v1.0 dated January 15, 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 evaluated configuration of the TOE includes the Ciena Carrier Ethernet Solutions 3900/5100 Series running Ciena Service Aware Operating System (SAOS) 6.14 product that is comprised of one or more of the product models listed in Table 2. The TOE also requires the 'advanced security' license in its evaluated configuration, to allow the TOE to operate as an SSH server for secure remote administration. The TOE includes all the code that enforces the policies identified (see Section 5).

The Non-FIPS mode of operation, Alarm Console, and Telnet remote administration is excluded from the evaluation. The Non-FIPS mode and Telnet remote administration will be disabled by configuration. 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.

TOE Introduction

Ciena Carrier Ethernet Solutions 3900/5100 Series is a network switch that receives data from an external source and forwards that data to one or many ports. The TOE is deployed as a Carrier Ethernet device. Carrier Ethernet provides a way to deliver Ethernet services across many networks while providing bandwidth management. CES operates on quality-of-service (QoS) capabilities and virtual switching functions to deliver different amounts of data to various ports. CES also contains next-generation Ethernet features that transport different Ethernet services through fiber or copper connections. CES hardware appliances run the Ciena Service Aware Operating System (SAOS) 6.14, with uniform security functionality between each of the hardware appliances.

The TOE consists of one or more models as specified in Section 4.2 below and includes the software version SAOS 6.14.

Physical Boundaries

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

Table 2 – Hardware Models and Specifications

Platform	3903 / 3904 / 3905	3916	3930-900/910	3931-900/910	3932 / 3930-930	3938 (Smart NID)	3942	5142	CN 5150	5160
1G/10G RJ-45	0	0	0	0	0	2	0	0	0	0
1G/10G SFP+	0	0	2	2	2	2	4	4	0	24
10/100/1000M RJ-45	0	0	0	4	0	8	0	0	0	0
100M/1G SFP	2	4	4	4	4	8	0	20	48	0
XFP	0	0	0	0	0	0	0	0	4	0
Combo RJ-45/SFP	3903 - 1 3904 - 2 3905 - 2	2	4	0	4	0	20	0	0	0
CPU	2x800 MHz ARM Cortex A9	2x500 MHz Cavium 5220	4x600 MHz Cavium 5230	2x600 MHz Cavium 5220	4x600 MHz Cavium 5230	6x1 GHz Cavium 6335	4x1 GHz Cavium 6230	6x1 GHz Cavium 6335	4x600 MHz Cavium 5230	6x1 GHz Cavium 6335
Ethernet Management Port	N	N	Y	N	Y	Y	Y	Y	Y	Y
Power Options	AC, DC	AC, DC	AC, DC (modular)	AC, DC (modular)	AC, DC (modular)	AC	AC, DC	AC, DC (modular)	AC, DC (modular)	AC, DC (modular)

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
Audit Server	A file server running the secure file transfer protocol (SFTP) that is used by the TOE to

Component	Usage/Purpose Description for TOE performance
	securely transmit audit data to a remote storage location.
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).
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

Security Audit

The TOE contains mechanisms to generate audit data to record predefined events on the TOE. Each audit record contains the user 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 is read-only for authorized administrators. Authorized administrators can securely transmit stored audit data to a remote storage location using SFTP.

Cryptographic Support

The TOE provides cryptography in support of SSH trusted communications. Asymmetric keys that used by the TSF are generated in accordance with NIST SP 800-56A. The TOE uses FIPS-validated cryptographic algorithms (see Table 4 for certificate references).

Table 4 FIPS References

Algorithm	Cert. #
AES	3522
RSA	1808
SHS	2904
HMAC	2250
DRBG	881

The TOE provides cryptography in support of remote administrative management via SSHv2. The cryptographic services provided by the TOE are described in Table below.

Table 5 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Secure Shell Establishment (SSH)	Used to establish initial SSH session.
AES	Used to encrypt SSH session traffic.
RSA Signature Services	Used in SSH session establishment. Update integrity verification
HMAC	Used for keyed hash, integrity services in SSH session establishment.
DRBG	Used for random number generation Used in SSH session establishment.
SHS	Used to provide SSH traffic integrity verification

User Data Protection

The TOE ensures that administrative traffic is isolated from data plane traffic through the use of VLANs. The TOE also 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.

Identification and Authentication

Users authenticate to the TOE as administrators 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. Users are authenticated either through a locally-defined username/password combination or through SSH public key-based authentication, depending on the configuration of the TSF and the method used to access the TOE. 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.

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. The Limited user is a read-only user, so any commands the user performs on the TOE will only allow the user to view different attributes and settings. The next level role is the Admin user who can perform all system configurations with the exception of managing users. Following the Admin role is the Super role. Super users can perform all system configurations including user management, including creating and deleting users on the TOE. 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.

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-512. 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 CLI. The TOE software version is administratively verifiable and software updates are signed to provide assurance of their integrity. The TSF also validates its correctness through the use of self-tests for both cryptographic functionality and integrity of the system software.

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 displays a configurable warning banner prior to use of the TSF.

Trusted Path/Channels

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

6 Documentation

The vendor provides guidance documentation:

- Ciena Carrier Ethernet Solutions 3900/5100 Series Supplemental Administrative Guide v1.0
- 39XX/51XX SAOS 6.14 Product Fundamentals - 009-3257-006
- 39XX/51XX SAOS 6.14 Administration and Security - 009-3257-006
- 39XX/51XX SAOS 6.14 Configuration - 009-3257-008
- 39XX/51XX SAOS 6.14 Command Reference - 009-3257-010
- Hardware Installation and Start-up Manuals – names vary based on individual hardware models, reference [1] for the full list
- 39XX/51XX SAOS 6.14 System Event Reference - 009-3257-024
- 39XX/51XX SAOS 6.14 Advanced Ethernet Configuration - 009-3257-040
- 39XX/51XX SAOS 6.14 Fault, Logging, and Performance Management - 009-3257-009
- 39XX/51XX SAOS 6.14 Advanced OAM Configuration - 009-3257-044
- 39XX/51XX SAOS 6.14 Software Management and Licensing - 009-3257-018
- 39XX/51XX SAOS 6.x Planning, Engineering, and Ordering Guide - 009-3299-029

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Ciena Carrier Ethernet Solutions 3900/5100 Series standalone network hardware appliances that run the Ciena Service Aware Operating System (SAOS) 6.14.

To use the product in the evaluated configuration, the product must be configured as specified in the *Ciena Carrier Ethernet Solutions 3900/5100 Series 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 Carrier Ethernet Solutions 3900/5400 Series" Evaluation Technical Report v1.0 dated January 15, 2016*, which is not publically available.

Test Configuration

The evaluation team configured each tested model of the TOE according the *Ciena Carrier Ethernet Solutions 3900/5100 Series 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 three models 3904, 3931-910 and 5142. This ensured that the firmware images were tested on each processor type (ARM and Cavium) to ensure the same results were produced. In addition the full suite of test assurance activities was divided up, in a non-overlapping manner, across four models to perform sample testing on the 3905, 5142, 5150 and 5160. In addition the different interface types and interface speeds were sampled to ensure the same results were produced.

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

- SFTP Server for audit export
- NTP Server to acquire the time

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

- WireShark: version 1.12.6
- Bitvise SSH Client: version 6.43

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

Developer Testing

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

Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Ciena CES 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.

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.
- CLI Privilege Escalation
  This attack involves enumerating a valid username with access to a non SAOS-CLI shell, then cracking the user's password and logging in.
- 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 CES 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.

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 CES 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.

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.

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.

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.

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.

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.

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 Carrier Ethernet Solutions 3900/5100 Series 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 Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0* dated January 7, 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 Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0, dated January 7, 2016
6. Ciena Carrier Ethernet Solutions 3900/5100 Series Supplemental Administrative Guide v1.0, dated December 18, 2015