National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Ciena Carrier Ethernet Solutions 3900/5100 Series

Report Number: CCEVS-VR-VID10921-2018
Version 1.0
March 26, 2019

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

Patrick Mallett, PhD.
The MITRE Corporation

Jean Petty
The MITRE Corporation

Common Criteria Testing Laboratory

Herbert Markle, CCTL Technical Director
Christopher Rakaczky
Dave Cornwell

Booz Allen Hamilton (BAH)
Laurel, Maryland

Table of Contents

1 EXECUTIVE SUMMARY 4
2 IDENTIFICATION 5
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE 6
4 ARCHITECTURAL INFORMATION 9
5 SECURITY POLICY 11
6 DOCUMENTATION 13
7 EVALUATED CONFIGURATION 14
8 IT PRODUCT TESTING 15
9 RESULTS OF THE EVALUATION 19
10 VALIDATOR COMMENTS 21
11 ANNEXES 22
12 SECURITY TARGET 23
13 LIST OF ACRONYMS 24
14 TERMINOLOGY 25
15 BIBLIOGRAPHY 26

Table 1 - Evaluation Identifiers 5
Table 2 - 3900 models 9
Table 3 - 5100 Models 9
Table 4 - IT Environment Components 10
Table 5 - Cryptographic Algorithm Table 11
Table 6 - Public Vulnerability Keyword Search 17

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 3900/5100 Series provided by Ciena Corp. 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 Laurel, Maryland, United States of America, and was completed in March 2019. 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 *collaborative Protection Profile for Network Devices Version 2.0 + Errata 20180314* (NDcPP).

The Target of Evaluation (TOE) Ciena Carrier Ethernet Solutions 3900/5100 Series. The TOE is a family of standalone network hardware appliances that run on the Ciena Service Aware Operating System (SAOS) 6.17 with uniform security functionality between each of the hardware appliances. The exception being that the 5170 model which runs SAOS 8.6.1. SAOS is a Linux-based operating system. 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. 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. The evaluated TOE functionality includes only the security functional behavior that is defined in the claimed NDcPP.

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 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 December 28, 2018 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 Compliant 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 results of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ciena Carrier Ethernet Solutions, running the SAOS software version 6.17 or 8.6.1 Refer to Table 2 and 3 for Model Specifications
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018, including all applicable NIAP Technical Decisions and Policy Letters
Security Target	Ciena Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0, dated December 28, 2018
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Ciena Corporation Carrier Ethernet Solutions 3900/5100 Series" Evaluation Technical Report v1.0 dated December 31, 2018
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, Laurel, Maryland
CCEVS Validators	Patrick Mallett, PhD., The MITRE Corporation Jean Petty, The MITRE Corporation

Table 1 - Evaluation Identifiers

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.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

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 network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
- **T.WEAK_CRYPTOGRAPHY –** Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
- **T.UNTRUSTED_COMMUNICATION_CHANNELS** – Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
- **T.WEAK_AUTHENTICATION_ENDPOINTS –** Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical

network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.

- **T.UPDATE_COMPROMISE –** Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
- **T.UNDETECTED_ACTIVITY** – Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
- **T.SECURITY_FUNCTIONALITY_COMPROMISE –** Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
- **T.PASSWORD_CRACKING –** Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
- **T.SECURITY_FUNCTIONALITY_FAILURE –** An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314*, 14 March 2018, 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 Security Target. All other functionality provided by these devices, needs to be assessed separately and no further conclusions can be drawn about their effectiveness. In particular, the CES's Quality of Service (QoS) and switching services described in Section 1.3 of the Security Target were not assessed as part of this evaluation. Further information of excluded functionality can be found in Section 2.3 of the Security Target.

The evaluated configuration of the TOE is the Ciena Carrier Ethernet Solutions 3900/5100 Series devices described in Table 2 and Table 3 running the SAOS software version 6.17 with the exception that model 5170 runs SAOS 8.6.1. The TOE also includes the ‘advanced security’ license in its evaluated configuration, which allows the TOE to operate as an SSH server. In the evaluated configuration, the TOE uses SSH to secure remote command-line administration. and TLS and SSH to secure transmissions of security-relevant data from the TOE to external entities such as authentication server, update server and syslog. The TOE includes administrative guidance in order to instruct Security 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.

4 Architectural Information

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

4.1 TOE Introduction

The TOE is a network device as defined in the NDcPP which states: "This is a Collaborative Protection Profile (cPP) whose Target of Evaluation (TOE) is a network device… A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.". The TOE consists of the Ciena Carrier Ethernet Solutions, running the SAOS software version 6.17 or 8.61. Thus, the TOE is a network device composed of hardware and software.

4.2 Physical Boundary

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

Platform	3903 / 3904 / 3905	3906	3916	3926M	3928	3930-900/910	3931-900/910	3932 / 3930-930	3942
10/100/1000M RJ-45	--	2	--	--	--	--	4	--	20
Combo RJ-45/SFP	3903 - 1 3904 - 2 3905 - 2	2	2	--	--	4	--	4	--
100M/1G SFP	2	2	4	2	8	4	4	4	--
1G/10G SFP+	--	--	--	6	4	2	2	2	4
CPU	2x800 MHz ARMv7 Cortex A9	2x800 MHz ARMv7 Cortex A9	2x500 MHz Cavium OCTEON 5220	4x1.5GHz ARM Cortex A53 AARCH64	4x1.5GHz ARM Cortex A53 AARCH64	4x600 MHz Cavium OCTEON 5230	2x600 MHz Cavium OCTEON 5220	4x600 MHz Cavium OCTEON 5230	4x1 GHz Cavium OCTEON II CN6230
Ethernet Management Port	N	Y	N	Y	Y	Y	N	Y	Y
Power Options	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC	AC, DC

Table 2 - 3900 models

Platform	5142	CN 5150	5160	5170
10/100/1000M RJ-45	--	--	--	--
Combo RJ-45/SFP	--	--	--	--
100M/1G SFP	20	48	--	--
1G/10G SFP+	4	--	24	40
XFP	--	4	--	--
100G	--	--	--	5170U - 4xQSFP28 5170H – 2xQSFP28/2xCFP4
CPU	6x800MHz Cavium OCTEON II CN6335	4x600MHz Cavium OCTEON 5230	6x800MHz Cavium OCTEON II CN6335	Intel Xeon D-1500
Ethernet Management Port	Y	Y	Y	Y
Power Options	AC, DC	AC, DC	AC, DC	AC, DC

Table 3 - 5100 Models

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

Component	Definition
Audit Server (SFTP Server)	A file server running the secure file transfer protocol (SFTP) that is used by the TOE to securely transmit audit data to a remote storage location.
Syslog Server	The Syslog Server connects to the TOE and allows the TOE to send Syslog messages to it for remote storage. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
Certification Authority	A server that acts as a trusted issuer of digital certificates and implements an OCSP responder to verify revocation status of a certificate.
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.
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.
RADIUS Server	A server providing centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service, i.e. external authentication mechanism. Communications are secured using TLS.

Table 4 - IT Environment Components

5 Security Policy

5.1.1 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 with the exception of a Security Administrator capable of deleting logs. Audit data can be securely transmitted to a remote storage location using SFTP or to a remote syslog server using TLS.

5.1.2 Cryptographic Support

The TOE provides cryptography in support of TLS and SSH trusted communications. Asymmetric keys that are used by the TSF are generated in accordance with FIPS PUB 186-4 and RFC 3526. Keys are established according to NIST SP 800-56A Revision 2, NIST SP 800-56B Revision 1 and RFC 3526.
The TOE uses software-based cryptography to provide cryptographic services using the OpenSSL FIPS Object Module (FOM) version 2.0.12 with CMVP certificate #1747. Both SAOS 6.17 and SAOS 8.6.1 use OpenSSL module 2.0.12.
The TOE uses FIPS-validated cryptographic algorithms to provide cryptographic services. The TOE uses CAVP-validated cryptographic algorithms to ensure that appropriately strong cryptographic algorithms are used for these trusted communications:

SFR	Algorithm Cert	CAVP Cert. #
FCS_COP.1/DataEncryption	AES	5419, 5665
FCS_CKM.2	CVL	1872, 2048
FCS_RBG_EXT.1	DRBG	2114, 2287
FCS_CKM.1, FCS_COP.1/SigGen	ECDSA	1440, 1531
FCS_COP.1/KeyedHash	HMAC	3589, 3770
FCS_CKM.1, FCS_COP.1/SigGen	RSA	2903, 3047
FCS_COP.1/Hash	SHS	4350, 4539

Table 5 - Cryptographic Algorithm Table

The TOE collects entropy from a source contained within the device to ensure sufficient randomness for secure key generation. Cryptographic keys are destroyed when no longer needed.

5.1.3 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, RADIUS, 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. When the configured amount of failed authentication attempts is reached, the user is locked out for configurable amount of time. The Super role can also manually unlock the user.

5.1.4 Security Management

The TOE maintains distinct roles for user accounts: Limited, Admin, and Super. These roles define the management functions authorized 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.
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, set the time, configure cryptographic functionality, view/edit audit data, and initiate updates. Following the Admin role is the Super role. An administrator with the Super role can perform all system configurations including user management, including creating and deleting users on the TOE, transferring audit data to a remote location. 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.

5.1.5 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 via its local hardware clock which is manually set by an administrator. 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.

5.1.6 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.

5.1.7 Trusted Path/Channels

A trusted path is established to the TOE using SSHv2 for remote administration. The TOE establishes trusted channels for sending audit data to remote syslog server, for downloading software updates, and authenticating to the RADIUS server. Audit logs are sent to a remote syslog server using TLS or using SFTP (FTP over SSH) to a remote audit server. An SSH trusted channel is established to download updates using SFTP from an update server. The trusted channel to the RADIUS server is protected by TLS.

6 Documentation

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

- Ciena Carrier Ethernet Solutions 3900/5100 Series Supplemental Administrative Guidance for Common Criteria - v1.0
- 39XX/51XX SAOS 6.17 Product Fundamentals - 009-3285-006
- 39XX/51XX SAOS 6.17 Administration and Security - 009-3285-007
- 39XX/51XX SAOS 6.17 Base Configuration - 009-3285-008
- 39XX/51XX SAOS 6.17 Command Reference - 009-3285-010
- 39XX/51XX SAOS 6.17 Software Management and Licensing - 009-3285-018
- 5170_SAOS_8.6.1_Product_Fundamentals StdRevA - 380-1877-010
- 5170_SAOS_8.6.1_Administration and Security StdRevA - 380-1877-301
- 5170_SAOS_8.6.1_Base Configuration StdRevA - 380-1877-310
- 5170_SAOS_8.6.1_Command Reference StdRevA - 380-1877-810
- 5170_SAOS_8.6.1_ Software Management and Licensing - 380-1877-221

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Ciena Carrier Ethernet Solutions, running the software: SAOS 6.17 or 8.6.1. Section 4.2 describes the TOE's physical configuration as well as the operational environment components to which it communicates. In its evaluated configuration, the TOE is configured to communicate with the following environment components:

- Certificate Authority/OCSP Responder
- RADIUS Server for remote authentication
- Management Workstation for local and remote administration
- Syslog Server for recording of syslog data
- Update server for receiving software updates

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 Guidance for Common Criteria - v1.0* 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 *Assurance Activities Report for Target of Evaluation Ciena Carrier Ethernet Solutions 3900/5100 Series Assurance Activities Report v1.0 dated December 31, 2018*.

8.1 Test Configuration

The evaluation team configured the TOE for testing according to the *Ciena Carrier Ethernet Solutions 3900/5100 Series Supplemental Administrative Guidance for Common Criteria - v1.0* (AGD) document. The evaluation team set up a test environment for the independent functional testing that allowed them to perform the assurance activities against the TOE over the SFR relevant interfaces. The evaluation team conducted testing between June and July 2018 at Ciena's Headquarters located in Hanover, MD and at the CCTL facility in Laurel, MD. Ciena's test environment was located on an isolated network. Testing was performed against all management interfaces defined in the ST (local CLI and remote CLI).

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
- RADSEC server for environmental authentication
- OCSP responder for certificate status checking

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

- WireShark: version 2.6.2
- Bitvise SSH Client: version 7.31
- PuTTY .70

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

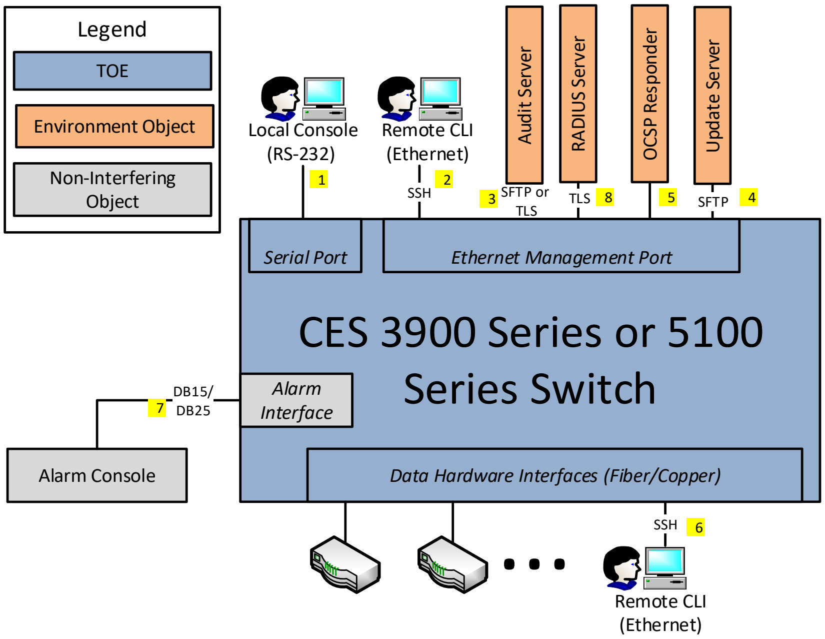

Figure 1 - Test Configuration

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 reviewed vendor documentation, formulated hypotheses, performed vulnerability analysis, and documented the hypotheses and analysis in accordance with the NDcPP requirements. Keywords were identified based upon review of the Security Target and AGD. The following keywords were identified:

Keyword	Description
Ciena	This is a generic term for searching for known vulnerabilities produced by the company as a whole.
Ciena Carrier Ethernet Solutions	This is a generic term for searching for known vulnerabilities for the product family.
3900 Series	This is a generic term for searching for known vulnerabilities for the product family.
5100 Series	This is a generic term for searching for known vulnerabilities for the product family.
SAOS	A specific version was not included in the search because this version may be within a range of vulnerable operating system versions and not listed separately.
OpenSSL 1.0.2j-fips	This is a generic term for searching for known vulnerabilities for the underlying cryptography module on the 3900 series. A specific version was not included in the search because this version may be within a range of vulnerable versions and not listed separately.
OpenSSL 1.0.2n-fips	This is a generic term for searching for known vulnerabilities for the underlying cryptography module on the 5100 series. A specific version was not included in the search because this version may be within a range of vulnerable versions and not listed separately.
OpenSSH 7.6p1	This is a generic term for searching for known vulnerabilities for the SSH module on the 5100 series. A specific version was not included in the search because this version may be within a range of vulnerable versions and not listed separately.
OpenSSH 7.5p1	This is a generic term for searching for known vulnerabilities for the SSH module on the 3900 series. A specific version was not included in the search because this version may be within a range of vulnerable versions and not listed separately.

Table 6 - Public Vulnerability Keyword Search

These keywords were used individually and as part of various permutations and combinations to search for vulnerabilities on public vulnerability sources on December 21, 2018. The public search was again update March 24, 2019 with no further vulnerabilities discovered. The following public vulnerability sources were searched:

- NIST National Vulnerabilities: https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/ https://www.cvedetails.com/vulnerability-search.php
- US-CERT: http://www.kb.cert.org/vuls/html/search
- SecurITeam Exploit Search: www.securiteam.com
- Tenable Network Security http://nessus.org/plugins/index.php?view=search
- Tipping Point Zero Day Initiative http://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities

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 an attempt to access the underlying OS 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

- Fuzzing – Mutated TYPE and CODE
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4, IPv6, ICMPv4, and ICMPv6 packets.

- Fuzzing – Mutated remaining field
  This test determines if the TOE is adversely affected by the handling of large number of mutated IPv4 and IPv6 packets where the header fields are carefully mutated to represent boundary cases, significant values, and randomly chosen values

- SSH Timing Attack (User Enumeration)
  This attack attempts to enumerate validate usernames for the SSH interface, by exploiting a vulnerability in OpenSSH as described in CVE-2018-15473.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.

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 Carrier Ethernet Solutions 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 validators 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 validators 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 Document related to the examination of the information contained in the operational guidance documents.

The validators 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 units. The evaluation team found that the TOE was identified.

The validators 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 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 validators 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 validators 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 Document, 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 Supplemental Administrative Guidance for Common Criteria Version 1.0* document. No versions of the TOE and software, either earlier or later were evaluated.

Administrators should take note of the fact that when the product is configured to offload audit files to an audit logging server, if that communications link is interrupted, the audit files generated during the time of the interruption will be captured locally. However, upon resumption of the connectivity, the offload begins with the reconnection and will NOT send those audit files generated during the outage. It will be necessary for the administrator to take steps to offload those files or they will be overwritten when the audit log is full.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Ciena Carrier Ethernet Solutions 3900/5100 Security Target v1.0,* dated December 28, 2018.

13 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CES	Carrier Ethernet Solutions
CSP	Critical Security Parameter
CTR	Counter (AES mode)
DHE	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
HMAC	Hashed Message Authentication Code
KAS	Key Agreement Scheme
MAC	Media Access Control
NDcPP	Collaborative Protection Profile for Network Devices
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
SSH	Secure Shell

14 Terminology

Term	Definition
Entropy	A string of quasi-random data that is generated by unpredictable physical and/or logical phenomena in a computer and is used in the generation of random numbers.
Security Administrator	The claimed Protection Profile defines a Security Administrator role that is authorized to manage the TOE and its data. The TOE maintains three administrator roles: Limited, Admin, and Super, each of which has certain authorizations to perform management functions on the TOE. A Security Administrator is a user who is attempting to perform a function that is allowed by their assigned administrative role. The use of ‘privilege’ is synonymous with the use of ‘role’ when discussing the administrator roles defined by the TOE.
Trusted Channel	An encrypted connection between the TOE and a trusted remote server.
Trusted Path	An encrypted connection between a remote administrative interface and 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. collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018
6. Ciena Carrier Ethernet Solutions 3900/5100 Series Security Target v1.0, dated December 28, 2018
7. Ciena Carrier Ethernet Solutions 3900/5100 Series Supplemental Administrative Guidance for Common Criteria - v1.0
8. 39XX/51XX SAOS 6.17 Product Fundamentals - 009-3285-006
9. 39XX/51XX SAOS 6.17 Administration and Security - 009-3285-007
10. 39XX/51XX SAOS 6.17 Base Configuration - 009-3285-008
11. 39XX/51XX SAOS 6.17 Command Reference - 009-3285-010
12. 39XX/51XX SAOS 6.17 Software Management and Licensing - 009-3285-018
13. 5170_SAOS_8.6.1_Product_Fundamentals Standard Revision A - 380-1877-010
14. 5170_SAOS_8.6.1_Administration and Security Standard Revision A - 380-1877-301
15. 5170_SAOS_8.6.1_Base Configuration Standard Revision A - 380-1877-310
16. 5170_SAOS_8.6.1_Command Reference Standard Revision A - 380-1877-810
17. 5170_SAOS_8.6.1_ Software Management and Licensing - 380-1877-221
18. Assurance Activity Report for a Target of Evaluation "Ciena Carrier Ethernet Solutions 3900/5100 Series" Assurance Activities Report v1.0 dated December 31, 2018