National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series, Version 10.5

Report Number: CCEVS-VR-VID10680-2016

Dated: January 28, 2015

Version: 1.0

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

Paul Bicknell

Jay Vora

The MITRE Corporation

Common Criteria Testing Laboratory

Pascal Patin

Anthony Busciglio

Acumen Security, LLC

Table of Contents

1 Executive Summary 5

2 Identification 6

3 Architectural Information 7

3.1 TOE Components 7
3.2 Component Physical Description 8
3.3 Example TOE Deployment 8

4 Security Policy 10

4.1 Security audit 10
4.2 Cryptographic Support 10
4.3 User Data Protection 10
4.4 Identification and Authentication 10
4.5 Security Management 11
4.6 Protection of the TSF 11
4.7 TOE Access 11
4.8 Trusted path/Channels 12

5 Assumptions, Threats & Clarification of Scope 13

5.1 Assumptions 13
5.2 Threats 13
5.3 Clarification of Scope 14

6 Documentation 15

7 TOE Evaluated Configuration 16

7.1 Evaluated Configuration 16
7.2 Excluded Functionality 16

8 IT Product Testing 17

8.1 Developer Testing 17
8.2 Evaluation Team Independent Testing 17

9 Results of the Evaluation 18

9.1 Evaluation of Security Target 18
9.2 Evaluation of Development Documentation 18
9.3 Evaluation of Guidance Documents 18
9.4 Evaluation of Life Cycle Support Activities 19
9.5 Evaluation of Test Documentation and the Test Activity 19
9.6 Vulnerability Assessment Activity 19
9.7 Summary of Evaluation Results 19

10 Validator Comments & Recommendations 21

11 Annexes 22

12 Security Target 23

13 Glossary 24
14 Bibliography 25

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in January 2016. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3.

The Target of Evaluation (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 U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

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(s) 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	Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3
Security Target	Security Target
Evaluation Technical Report	VID 10680 Common Criteria NDPP Assurance Activity Report, version 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Paul Bicknell, Jay Vora

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target. The subsections below provide an overview of the Target of Evaluation (TOE).

3.1 TOE Components

The Cisco ONS and NCS 2000 Series includes the one or more of the following Chassis (Shelves):

- ONS:
  - 15454-M2
  - 15454-M6
- NCS 2000 Series
  - NCS 2002
  - NCS 2006
  - NCS 2015

Each of the Chassis support the following cards, except where specifically noted. In the evaluated configuration the chassis must include at least one controller card, at least one encryption care and at least one line card.

- Controller Cards (Management) (one or more):
  - 15454-M-TNC-K9
  - 15454-M-TSC-K9
  - 15454-M-TNCE-K9
  - 15454-M-TSCE-K9
  - NCS2K-TNCS-O-K9
  - NCS2K-TNCS-K9 (only supported on the NCS 2015 chassis)
- Encryption Cards (Data Traffic traversing the TOE):
  - 15454-M-WSE-K9
  - NCS2K-MR-MXP-LIC
  - Pluggable optics used
    - ONS-SC+-10G-SR=
    - CPAK-100G-SR10
    - QSFP-4x10G-LR-S=
- Line Cards (Data Traffic traversing the TOE; no encryption):
  - 15454-M-10X10G-LC
  - NCS2K-200G-CK-LIC=

The software is comprised of the Cisco's ONS/NCS 10.5 Release software version that consists of two images; MSTPR and NCS2K. The only difference in the software images is the new ROADM cards are only supported in NCS2K packages and the older Transponder cards are only supported in MSTP packages. The differences in the cards do not affect any of the security claims or any of the security functional requirements that are claimed in this Security Target. While these cards are the controllers cards that are used to manage the TOE, the difference are simply how the data that transverse the TOE is transmitted. All of the TOE management and

administrative traffic is protected and secured using HTTPS/TLS. All of the security management functions are the same in both packages.

The TOE is managed using the Cisco Transport Controller (CTC) management software that is installed on a Management Workstation (depicted as Admin Console in the figure below) during the setup and installation of the TOE. The CTC is a web-based graphical user interface (GUI) application capable of managing all of the security functions, as well as performing the provisioning and administration functions of the Controller Card.

3.2 Component Physical Description

The Cisco ONS 15454 M2 chassis has one slot for the control card and two slots for service cards. These two line-card slots provide increased power and cooling capability and a usable high-speed backplane for future applications. The M2 chassis can be configure with integrated DC or AC power inputs. With its front-facing connections, the M2 is ideal for cabinet installations and ETSI front-connection requirements, making this platform truly global.

The Cisco ONS 15454 M6 chassis has two slots for redundant control cards and six slots for service cards. These six line card slots provide increased power and cooling capability and a high-speed backplane for card-to-card interconnection. The M6 chassis can be configured with integrated and redundant DC or AC power inputs or a single power module for low-power and low-cost configurations.

The Cisco NCS 2015 has 15 slots for service cards and is 14 rack units (14RU) high, allowing three chassis to fit into one standard rack. The Cisco NCS 2015 chassis support AC or DC power applications. Four slots accommodate up to four power modules in a 3 + 1 redundant configuration, which is common in the NCS 2000 Series.

The Cisco NCS 2006 chassis is 6RU and has 6 slots for service cards. The Cisco NCS 2006 chassis can be configured with DC or AC power inputs. At 6 Rack Unit (RU) with 6 service slots, the Cisco NCS 2006 chassis is versatile. Metro/edge locations can minimize footprint while still accommodating multiple ROADM degrees and/or service line cards, and large core nodes can scale as large as necessary by using multishelf configurations.

The NCS 2002 is 2RU and has 2 slots for service cards. The NCS 2002 features 1 slot for the control card and 2 slots for service cards. The NCS 2002 can be configured with a single DC or AC power module.

3.3 Example TOE Deployment

All of the appliances included in the TOE implement the security functions the same way and implement the same set of security functions and SFRs; the difference between the different models is related to performance and/or other non-security relevant factors.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

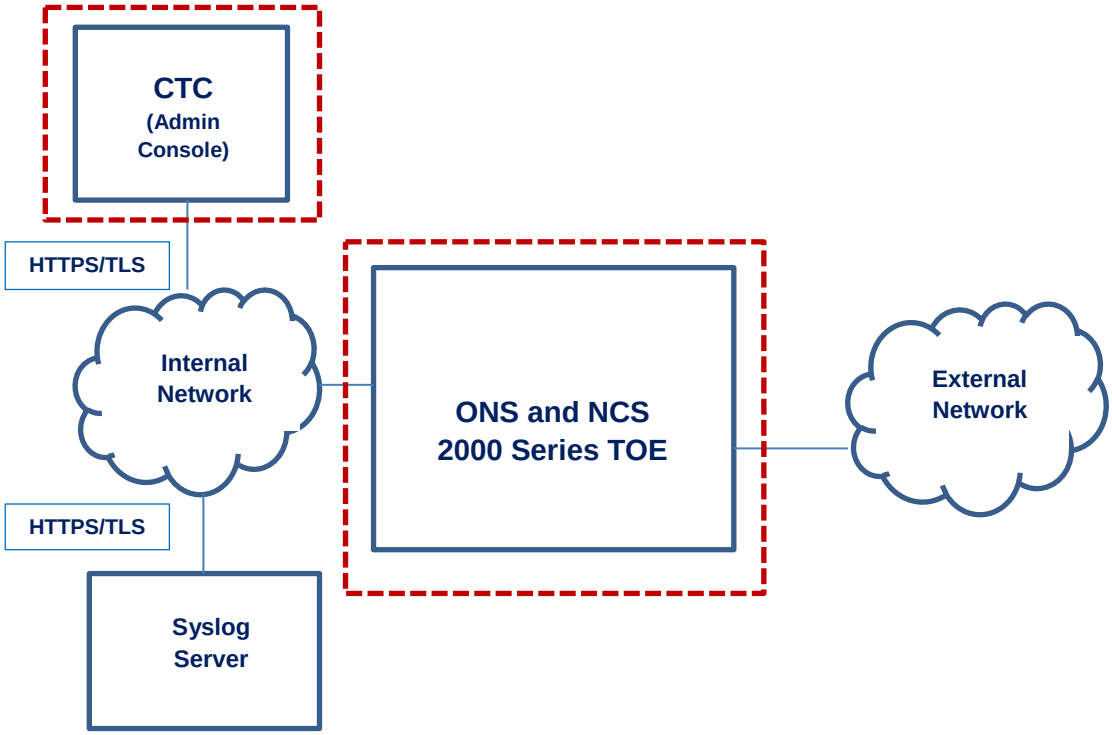

Figure 1 TOE Example Deployment

4 Security Policy

The TOE is comprised of several security features, as identified below.

- Security Audit
- Cryptography Support
- User Data Protection
- Identification & Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

In addition, the TOE implements all RFCs of the NDPP as necessary to satisfy testing/assurance measures prescribed therein. The security features of the TOE are described in more detail in the subsections below.

4.1 Security audit

The Cisco ONS and NCS 2000 Series provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco ONS and NCS 2000 Series generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. Auditing is always on to audit all events and therefore the administrator is only coupled with the management of the audit data storage and archive of the log files. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are archived over secure HTTPS/TLS connection to an external audit server.

4.2 Cryptographic Support

The TOE provides cryptography in support of HTTPS/TLS and TLS connections for remote administrative management and transmission of syslog records, respectively.

4.3 User Data Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

4.4 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters, password expiration as well as mandatory password complexity rules. The TOE

provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection.

4.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE; and
- Update to the TOE.

4.6 Protection of the TSF

The TOE protects the communications between the CTC and the node using TLS for a secure connection. The TOE also protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally Cisco ONS and NCS 2000 Series is not a general-purpose operating system and access to Cisco ONS and NCS 2000 Series memory space is restricted to only Cisco ONS and NCS 2000 Series functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. The TOE may also be configured to synchronize time with an NTP server.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

4.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also be configured to display an Authorized Administrator specified banner on the GUI management interface prior to accessing the TOE.

4.8 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over HTTPS and initiates secure HTTPS connections to transmit audit messages to remote syslog servers.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Assumption	Assumption Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5.2 Threats

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

Threat	Threat Definition
Reproduced from the U.S. Government Protection Profile for Security Requirements for Network Devices	
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.

Threat	Threat Definition
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.

5.3 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 U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) with Errata #3.
- 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series Security Target [ST], version 1.0;
- Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series Operational User Guidance and Preparative Procedures [AGD], version 1.0;

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE consists of one or more physical devices including the controller, encryption and line cards and software as described below.

- Chassis (one or more):
  - 15454-M2
  - 15454-M6
  - NCS 2002
  - NCS 2006
  - NCS 2015
- Controller Cards (Management) (one or more):
  - 15454-M-TNC-K9
  - 15454-M-TSC-K9
  - 15454-M-TNCE-K9
  - 15454-M-TSCE-K9
  - NCS2K-TNCS-O-K9
  - NCS2K-TNCS-K9 (only supported on the NCS 2015 chassis)
- Encryption Cards (Data Traffic traversing the TOE):
  - 15454-M-WSE-K9
  - NCS2K-MR-MXP-LIC
  - Pluggable optics used
    - ONS-SC+-10G-SR=
    - CPAK-100G-SR10
    - QSFP-4x10G-LR-S=
- Line Cards (Data Traffic traversing the TOE; no encryption):
  - 15454-M-10X10G-LC
  - NCS2K-200G-CK-LIC=
- CTC Management
- Software
  - ONS/NCS 10.5 Release software version

7.2 Excluded Functionality

The following functionality is excluded from the evaluation.

Excluded Functionality	Exclusion Rationale
Non-FIPS 140 mode of operation	This mode of operation includes non-FIPS mode operations.

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices, version 1.1, June 8, 2012, with Errata#3.

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for the Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series, which is not publically available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

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

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publically available, and is not duplicated here.

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that 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 Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

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 Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series 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 NDPP.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 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 Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to

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

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 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 Test Documentation and the Test Activity

The evaluation team applied each EAL 1 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 and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it

demonstrates that the evaluation team performed the Assurance Activities in the NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators have no further comments about the evaluation results.

11 Annexes

Not applicable.

12 Security Target

Please see the Cisco Optical Networking Solution (ONS) and Network Convergence System (NCS) 2000 Series Security Target [ST], version 1.0.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 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.