National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Ciena Waveserver 5 OS R2.3.12

Report Number: CCEVS-VR-VID11390-2023

Dated: 12/06/2023

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Lauren Brandt

Jenn Dotson

Sheldon Durrant

Anne Gugel

Clare Parran

Richard (Rip) Toren

Common Criteria Testing Laboratory

Furukh Siddique

Toan Truong

Intertek, USA

Table of Contents

List of Tables

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 3 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 Ciena Waveserver 5 OS R2.3.12 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 Intertek in December 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Intertek. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the NDcPP v2.2e.

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR 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 ETR 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 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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 TOE: the fully qualified identifier of the product as evaluated.
- The 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.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Ciena Waveserver 5 OS R2.3.12
Protection Profile	Collaborative Protection Profile for Network Devices, version 2.2e [NDcPP v2.2e]
Security Target	Ciena Waveserver 5 OS R2.3.12 Security Target version 1.8
Evaluation Technical Report	Evaluation Technical Report for Ciena Waveserver 5 OS R2.3.12, version 0.8
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Ciena Corporation
Developer	Jian Gong
Common Criteria Testing Lab (CCTL)	Acumen Security 2400 Research Blvd. #395 Rockville, MD 20850
CCEVS Validators	Lauren Brandt, Jenn Dotson, Sheldon Durrant, Clare Parran, Anne Gugel, Richard (Rip) Toren

Table 1: Evaluation Identifiers

3 Assumptions, Threats & Clarification of Scope

3.1 Assumptions

The specific conditions listed in the following table 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.

ID		Assumption
A.PHYSICAL_PROTECTION		The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY		The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

ID		Assumption
A.NO_THRU_TRAFFIC_PROTECTION		A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR		The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES		The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

ID		Assumption
A.ADMIN_CREDENTIALS_SECURE		The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION		The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 2: Assumptions

3.2 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:

ID	Threat
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 tunnelling 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

ID	Threat
	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.

Table 3: Threats

3.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the NDcPP v2.2e, Version 3.1, Section 5.
- Consistent with the expectations of the PP, 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.

4 Architectural Information

The Ciena Waveserver 5 is a purpose-built, data center interconnect (DCI) platform designed to facilitate high-speed, high-capacity connections between data centers. This platform has been designed to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP 2.2e]. The Waveserver 5 incorporates a range of advanced security features to ensure the integrity and confidentiality of network communications. The TOE uses a Marvell CN9130 processor.

While not an exhaustive list, some the main security mechanisms being leveraged include the following.

1. Encrypted SSH Administration: The device supports encrypted SSH connections for secure remote administration, protecting the communication channel between administrators and the device from unauthorized access and eavesdropping.
2. RADIUS via TLS: The Waveserver 5 is capable of using RADIUS authentication with TLS encryption, ensuring the secure transmission of login credentials and providing an added layer of protection for user authentication.
3. Encrypted Syslog Traffic: The platform can encrypt syslog traffic via TLS to a syslog server, safeguarding the privacy and confidentiality of logs and preventing unauthorized access to sensitive log data.
4. NTP with SHA Authentication: The Waveserver 5 supports the use of NTP with SHA authentication, providing a secure method for time synchronization across network devices and reducing the risk of time-based attacks.

These highlighted security mechanisms, along with other measures, contribute to the Waveserver 5's ability to not only meet the collaborative Protection Profile for Network Devices, Version 2.2e, but also deliver a comprehensive and secure networking solution for end users.

5 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, summarized below.

Security Audit

The TOE generates audit events for all start-up and shut-down functions, and all auditable events as specified in Table 11 of the ST. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external syslog server using TLS v1.1 or TLS v1.2 protocol. Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event. The syslog server supports the following severity levels: emergency, alert, error, warning, notice, info and debug. In order to enable the logging to syslog server, a user must be logged in with an administrative access privilege and provision the settings to use a syslog server.

Cryptographic Support

The TOE leverages Waveserver 5 Cryptographic Library for all cryptographic services. The related CAVP validation details are provided in Security Target document Table 13. All algorithms claimed have CAVP certificates. The operating system is Linux Kernel v4.14. The TOE leverages the Waveserver 5 Cryptographic Library for its cryptographic functionality.

Identification and Authentication

The TOE supports Role Based Access Control. All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication and public key-based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration.
- Remote CLI administration via SSHv2 and HTTPS/TLS.
- Timed user lockout after multiple failed authentication attempts.
- Password configurations.
- Role Based Access Control – Superuser (Security Administrator), Admin and limited user.
- Configurable banners to be displayed at login.
- Timeouts to terminate administrative sessions after a set period of inactivity.

- Protection of secret keys and passwords.

TOE Access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after 10 minutes of session inactivity. An administrator can terminate their GUI session by clicking on the logout button. A user can terminate their local CLI session and remote CLI session by entering exit at the prompt.

Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Passwords are stored in encrypted format. Passwords are stored as SHA-512 salted hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE maintains the date and time by the setting of the time manually by a security administrator or by synchronizing with an NTP server configured by a security administrator.

Trusted Path/ Channel

The TOE supports TLS v1.1 or TLS v1.2 for secure communication to the following IT entities:

Syslog server and Radius server. The TOE supports HTTPS/TLS (WebUI) and SSH v2 (remote CLI) for secure remote administration.

6 Documentation

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

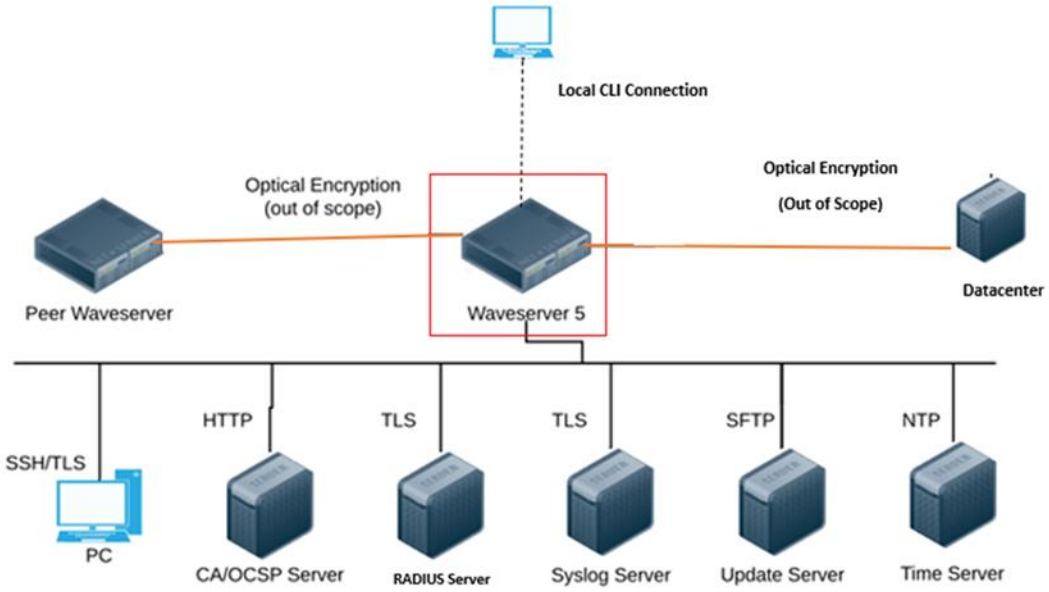
- Ciena Waveserver 5 OS R2.3.12 Security Target version 1.8 [ST]
- Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document, version 1.3 [AGD]

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE boundary is the hardware appliance, which is comprised of hardware and software components. It is deployed in an environment that contains the various IT components as depicted in the figure below.

The TOE is shipped with the software pre-installed on it. Software updates are available for download from the Ciena website.



7.2 Excluded Functionality

- Peer Waveserver is used for communication over the optical network and protected via encryption. This connection is not part of the evaluated configuration.
- The following interfaces are not in scope of the evaluation:
  - NETCONF
  - gRPC
  - RESTCONF
  - Swagger
  - FTP

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for Waveserver 5, which is not publicly available. The AAR 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 to the vendor-provided guidance documentation and ran the tests specified in the NDcPP version 2.2.e. The Independent Testing activity is documented in the AAR, which is publicly 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 ETR. The reader of this document can assume that all 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 Revision 5 and CEM version 3.1 Revision 5. The evaluation determined the Waveserver 5 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

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 Waveserver 5 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 NDcPP v2.2e.

The Validation team 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 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP v2.2e related to the examination of the information contained in the TOE Summary Specification.

The Validation team 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 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 NDcPP v2.2e related to the examination of the information contained in the operational guidance documents.

The Validation team 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 ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team 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 ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the NDcPP v2.2e and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team 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 v2.2e, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

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 Validation team 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 NDcPP v2.2e 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 NDcPP v2.2e and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Ciena Waveserver 5 Rel 2.3.12 Common Criteria Configuration Guide, Version 1.3. No versions of the TOE and software, either earlier or later were evaluated.

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. Section 1.4 of the ST defines product functionality not included in the scope of the evaluation. It is important to understand that connections between the TOE and a peer Waveserver device as well as connections between the TOE and the datacenter are over an encrypted optical network connection which is not included in the evaluated configuration. Therefore, these connections have not been evaluated through the NIAP certification process. In addition, the following interfaces are not in scope of the evaluation and have not been NIAP certified: NETCONF, gRPC, RESTCONF, Swagger, FTP and SFTP with the Update Server. Customers must use this functionality at their own risk. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Ciena Waveserver 5 OS R2.3.12 Security Target version 1.8

13 Glossary

The following definitions are used throughout this document:

Term	Definition
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.

Table 4: Glossary

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 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Collaborative Protection Profile for Network Devices Version 2.2e
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Ciena Waveserver 5 OS R2.3.12, version 0.8
7. Ciena Waveserver 5 Rel 2.3.12 Common Criteria Guidance Document, version 1.3
8. Ciena Waveserver 5 OS R2.3.12 Security Target version 1.8
9. Assurance Activity Report for Ciena Waveserver 5 OS R2.3.12, version 1.8
10. Test Plan for the Ciena Waveserver 5, version 1.4
11. Vulnerability Assessment for Ciena Waveserver 5, version 1.5