Certification Report

EAL 3 Evaluation of

nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTellect™ 2000

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-35
Version:	1.0
Date:	16 May 2005
Pagination:	i to iii, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.2*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment (CSE), or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the CSE, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment (CSE).

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 16 May 2005, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/en/services/common_criteria/trusted_products.html

This certification report makes reference to nCircle, IP360 and nTellect which are trademarks or registered trademarks of nCircle™ Network Security, Inc..

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTellect™ 2000; hereafter referred to as the nCircle™ IP360™ Vulnerability Management System V6.3.4, from nCircle™ Network Security, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation.

The nCircle™ IP360™ Vulnerability Management System V6.3.4 is a vulnerability management system designed to monitor a network and assess in real time the vulnerabilities of the IP enabled devices that are linked to it. It is designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 11 May 2005, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for the nCircle™ IP360™ Vulnerability Management System V6.3.4, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the nCircle™ IP360™ Vulnerability Management System V6.3.4 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report[1] for this product provide sufficient evidence that it meets the EAL 3 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 r256*.

The Communications Security Establishment, as the CCS Certification Body, declares that the nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTellect™ 2000 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list.

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of the Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 evaluation is the nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTellect™ 2000; hereafter referred to as nCircle™ IP360™ Vulnerability Management System V6.3.4, from nCircle™ Network Security, Inc.

2 TOE Description

The nCircle™ IP360™ Vulnerability Management System V6.3.4 is a vulnerability management system designed to monitor a network and assess in real time the vulnerabilities of the IP enabled devices that are linked to it. The nCircle™ IP360™ Vulnerability Management System V6.3.4 is designed to be installed and used in an environment that is configured and controlled in accordance with administrator guidance that is supplied with the product.

The nCircle™ IP360™ Vulnerability Management System V6.3.4 consists of the three physical components listed below:

- Vulnerability and Exposures Manager (VnE)
- Device Profiler (DP)
- nTellect™ (which is an optional component)

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the nCircle™ IP360™ Vulnerability Management System V6.3.4 is identified in Section 5 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title:	nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTelect™ 2000 Security Target
Version:	2.1
Date:	11 May 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 r256*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 r256*, incorporating all final interpretations issued prior to 7 October 2004.

The nCircle™ IP360™ Vulnerability Management System V6.3.4 is:

a. Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2; and

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3.

6 Security Policy

Security Management

The administrator and restricted user (when given permission by the administrator) are provided with a Graphic User Interface (GUI) to perform configuration and troubleshooting tasks. Restricted users are assigned privileges as determined by the administrator as per the security policy defined in the ST (Restricted User SFP (RU_SFP)). Alternatively, the VnE CLI (Command Line Interface) administrator and the DP/nTellect™ CLI administrator can perform configuration tasks using the CLI Interface. The TOE maintains four roles, which can be further specified based on very granular privilege controls in the VnE: administrator, restricted user, VnE CLI admin, and DP/nTellect™ CLI admin.

7 Assumptions and Clarification of Scope

Consumers of the nCircle™ IP360™ Vulnerability Management System V6.3.4 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of the product.

7.1 Secure Usage Assumptions

The secure usage assumptions and security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed are addressed in the Security Target. It is assumed that the product will be installed and configured using the guidance documents provided by nCircle™ Network Security, Inc. The security procedures that the consumer must carry out to configure the system such that the TOE is setup in the CC mode of operation are documented in the guidance documents (listed in Section 10).

7.2 Environmental Assumptions

The TOE hardware and software critical to security policy enforcement are assumed to be within controlled access facilities that will prevent unauthorized physical access and modification by potentially hostile outsiders. The administrator is responsible for ensuring that the assumptions and all the environmental objectives listed in Section 3 and Section 4 of the Security Target document are met in the deployed environment.

Some of the TOE self-protection (e.g., against physical tampering) is ensured by its environment. In particular, it is assumed that the TOE will remain attached to the physical connections made by a TOE user so that the TOE cannot be bypassed. Each IP360™ appliance is completely self-contained in that the hardware, operating system and applications provide all the services necessary to implement the TOE.

7.3 Clarification of Scope

The nCircle™ IP360™ Vulnerability Management System V6.3.4 can not prevent authorized administrators from carelessly configuring the system such that the TOE is not setup in CC mode of operation.

8 Architectural Information

The TOE comprises of the following functional components:

1. Graphical User Interface (GUI) – the VnE GUI encapsulates the functionality to manage the TOE. The GUI is accessible via a web browser with TLS enabled.

2. Device Profiler – performs network scanning at the request of the VnE. The profiling functionality is not a TSP enforcing component of the TOE.

3. nTellect™ - analyzes information from specific IP enabled devices on the target network. The analysis functionality is not a TSP enforcing component of the TOE.

4. Command Line Interface (CLI) – a command line interface exists for each device that encapsulates the functionality of configuring said device.

5. Events – the events component of the VnE is responsible for generating alerts and handling events such as trouble state reporting.

6. Reporting – the reporting component of the VnE is responsible for generating reports on scan results.

7. Upgrade - encapsulates the functionality of downloading upgrades from the software repository, and processing and installing the downloaded packages.

9 Evaluated Configuration

The evaluated configuration of the TOE is:

TOE Component	Operating System	Software Version	Hardware
Vulnerability and Exposures Manager (VnE)	FreeBSD v4.7	nCircle™ IP360™ Vulnerability Management System V6.3.4	VnE 1000 and VnE 3000
Device Profiler (DP)	FreeBSD 4.9	nCircle™ IP360™ Vulnerability Management System V6.3.4	DP 1000 and DP 2000
nTellect™	FreeBSD 4.9	nCircle™ IP360™ Vulnerability Management System V6.3.4	nTellect™ 2000

The publication entitled *nCircle™ IP360™ Vulnerability Management System V6.3.4 Settings Required for CC Mode of Operation* describes the procedures necessary to install and operate a nCircle™ IP360™ Vulnerability Management System V6.3.4 in its evaluated configuration.

10 Documentation

In addition to the document that describes the CC Mode Settings, nCircle™ Network Security, Inc. provides release notes, a Quick Start Guide for each appliance, a Basics Guide, an Administration Guide, and an Appliance Communication document.

The documents listed below are all available to consumers:

a. nCircle IP360™ Vulnerability Management System V6.3.4 Settings Required for CC Mode of Operation, Version 0.5, 29-Apr-05;
b. IP360 Release Notes, 28-Mar-05;
c. nCircle™ IP360 6.3 Quick Start Guide, 29-Mar-05;
d. nCircle™ IP360 6.3™ Device Profiler Quick Start Guide, 29-Mar-05;
e. nCircle™ IP360 6.3 IDS nTellect Quick Start Guide , 29-Mar-05;
f. nCircle™ IP360 6.3 Basics Guide, 29-Mar-05;
g. nCircle™ IP360 6.3 Administrator Guide, 29-Mar-05; and
h. nCircle™ IP360 6.3.0 Appliance Communication, 29-Sep-04.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the nCircle™ IP360™ Vulnerability Management System V6.3.4, including the following areas:

Configuration management: An analysis of the nCircle™ IP360™ Vulnerability Management System V6.3.4 development environment and associated documentation was performed. The evaluators found that the nCircle™ IP360™ Vulnerability Management System V6.3.4 configuration items were clearly marked and that control was exercised over all modifications to the configuration items. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the nCircle™ IP360™ Vulnerability Management System V6.3.4 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the nCircle™ IP360™ Vulnerability Management System V6.3.4 functional specification and high-level design. The evaluators determined that the design documents were internally consistent, and completely and accurately described all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the nCircle™ IP360™ Vulnerability Management System V6.3.4 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the nCircle™ IP360™ Vulnerability Management System V6.3.4 design and implementation.

Vulnerability assessment: The strength of function claim made in the Security Target for the nCircle™ IP360™ Vulnerability Management System V6.3.4 was validated. Additionally, evaluators assessed the developer's vulnerability analysis for completeness.

All the above listed evaluation analysis activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing independent vulnerability tests. During this evaluation, the evaluators developed their independent tests by examining the design and guidance documentation, examining developer analysis, and repeating a sub-set of developer tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer met their testing responsibilities by examining their test evidence, reviewing their test results, witnessing a subset of testing on site and repeating a subset of the developer tests.

The evaluators reviewed the developer's analysis of test coverage and depth and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and high-level design (HLD) was complete.

The subset of the developer tests that were repeated was selected based on the following:

a. TOE Summary Specification (TSS) coverage;
b. Security Functional Requirement (SFR) coverage;
c. HLD sub-system coverage;
d. Tests of interest; and
e. Random selection.

Developer's test cases were witnessed/repeated during the site visit and tests were repeated by the evaluator during independent testing.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

12.3 Independent Vulnerability Testing

The evaluators devised a set of penetration tests based on the developer's vulnerability analysis. Vulnerabilities assessed as potentially exploitable by an attacker possessing a low attack potential were used to develop penetration test cases.

The following potential attack areas were assessed during the development of potential attack scenarios:

a. Generic vulnerabilities;
b. Bypassing;
c. Tampering;
d. Direct attacks; and
e. Misuse.

At least one penetration attack and in most cases multiple attacks were developed for each of these areas. A total of 16 penetration attacks were developed and exercised against the TOE.

Penetration testing did not uncover any exploitable vulnerabilities for the nCircle™ IP360™ Vulnerability Management System V6.3.4 in the anticipated operating environment.

12.4 Conduct of Testing

The nCircle™ IP360™ Vulnerability Management System V6.3.4 was subjected to a comprehensive suite of formally-documented, independent, functional and vulnerability tests. The testing took place at the IT Security Evaluation and Testing (ITSET) facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. The CCS Certification Body witnessed a portion of the independent testing.

The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in the ETR[2].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the nCircle™ IP360™ Vulnerability Management System V6.3.4 behaves as specified in the ST and functional specification.

[2] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 3** level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The nCircle™ IP360™ Vulnerability Management System V6.3.4 includes comprehensive guides for the installation, configuration and operation of the VnE, Device Profiler, and nTellect™ components. The publication entitled *nCircle™ IP360™ Vulnerability Management System V6.3.4 Settings Required for CC Mode of Operation* describes all of the procedures necessary to install and operate a nCircle™ IP360™ Vulnerability Management System V6.3.4 in its evaluated configuration.

15 Glossary

This section expands any acronyms, abbreviations and initializations used in this report.

15.1 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CR	Certification Report
CSE	Communications Security Establishment
DP	Device Profiler
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
VnE	Vulnerability and Exposures Manager

16 References

This section lists all documentation used as source material for this report:

a. Common Criteria for Information Technology Security Evaluation, Version 2.2 r256, January 2004; Parts 2 and 3 (aligned with ISO/IEC 15408:2004).

b. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, January 2004, Version 2.2 Revision 256, CCIMB-2004-01-004.

c. CCS #4: Technical Oversight for TOE Evaluation, Canadian Common Criteria Evaluation and Certification Scheme (CCS), Version 1.0, October 3, 2002.

d. nCircle™ IP360™ Vulnerability Management System V6.3.4 Vulnerability and Exposure Manager (VnE 1000 and VnE 3000) Device Profiler (DP 1000 and DP 2000) nTelect™ 2000 Security Target, Version 2.1, 11 May 2005.

e. Evaluation Technical Report (ETR), nCircle™ IP360™ Vulnerability Management System V6.3.4, EAL 3 Evaluation, Common Criteria Evaluation Number, 383-4-35, Document No. 1489-000-D002, Version 1.2, 11 May 2005.