Certification Report

EAL 3+ Evaluation of

NetScout nGenius® InfiniStream® (V4.7 MR2), nGenius® Performance Manager (V4.7 MR2), and nGenius® K2 (V4.7 MR2)

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-109-CR
Version: 1.0
Date: 4 June 2010
Pagination: i to iii, 1 to 12

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 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 Canada, 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 Communications Security Establishment Canada, 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 Canada.

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/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration 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 DOMUS IT Security Laboratory located in Ottawa, Canada.

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) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 4 June 2010, 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 and the Common Criteria Portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarked or registered trademarks:

- NetScout, nGenius and InfiniStream are registered trademarks of NetScout Systems, Inc.

TABLE OF CONTENTS

Executive Summary

The nGenius® InfiniStream® Version 4.7 MR2, nGenius Performance Manager Version 4.7 MR2, and nGenius K2 Version 4.7 MR2 (hereafter referred to as nGenius Service Assurance Solution V4.7 MR2), from NetScout Systems, Inc. is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

The nGenius Service Assurance Solution V4.7 MR2 is a unified service delivery management platform which provides comprehensive, real-time network, application and service performance intelligence to ensure optimized network operation. The nGenius Service Assurance Solution V4.7 MR2 provides network visibility with a common data set of service-oriented analysis and reporting functions that also promote collaboration with team-oriented workflows.

The nGenius Service Assurance Solution V4.7 MR2 provides a unified approach to managing service delivery which allows customers to optimize the service delivery, protect network application performance and simplify operations.

DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 28 April 2010 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 nGenius Service Assurance Solution V4.7 MR2, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in 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 (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2*. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the nGenius Service Assurance Solution V4.7 MR2 evaluation meets all the conditions

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

of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products List (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is nGenius® InfiniStream® Version 4.7 MR2, nGenius Performance Manager Version 4.7 MR2, and nGenius K2 Version 4.7 MR2 (hereafter referred to as nGenius Service Assurance Solution V4.7 MR2), from NetScout Systems.

2 TOE Description

The nGenius Service Assurance Solution V4.7 MR2 is a unified service delivery management platform which provides comprehensive, real-time network, application and service performance intelligence to ensure optimized network operation. The nGenius Service Assurance Solution V4.7 MR2 provides network visibility with a common data set of service-oriented analysis and reporting functions that also promote collaboration with team-oriented workflows.

The nGenius Service Assurance Solution V4.7 MR2 provides a unified approach to managing service delivery which allows customers to optimize the service delivery, protect network application performance and simplify operations.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the nGenius Service Assurance Solution V4.7 MR2 is identified in Section 1.5.3 of the Security Target (ST).

4 Security Target

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

Title: NetScout Systems, Inc. nGenius® InfiniStream (V4.7 MR2), nGenius® Performance Manager (V4.7 MR2), and nGenius® K2 (V4.7 MR2) Security Target

Version: 14.0

Date: 6 April 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version3.1 Revision 2*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.*

The nGenius Service Assurance Solution V4.7 MR2 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;
b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

The nGenius Service Assurance Solution V4.7 MR2 implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information about monitored networks and systems; details of these security policies can be found in Section 6 of the ST.

In addition, the nGenius Service Assurance Solution V4.7 MR2 implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the nGenius Service Assurance Solution V4.7 MR2 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The Administrator will install and configure the TOE according to the administrator guidance and specific organizational security policies.
- Administrators are non-hostile and follow the administrator guidance when using the TOE. Administration is competent and on-going.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE will be located in an environment that provides physical security, uninterruptible power, and temperature control required for reliable operation.

- The TOE will be located behind a firewall and an Access Control List (ACL) will be created on the router between the TOE and the rest of the network to provide network security.

- There will be a network that supports communication between distributed components of the TOE. This network functions properly.

7.3 Clarification of Scope

The nGenius® Service Assurance Solution V4.7 MR2 was designed and intended for use in a structured corporate environment. It cannot prevent authorized administrators from carelessly configuring the TOE such that the TOE security is compromised.

The nGenius Service Assurance Solution V4.7 MR2 provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community. While it is designed to protect its user community against inadvertent or casual attempts to breach system security, it is not intended for situations in which determined attempts by hostile and well-funded attackers use sophisticated attacks from within the physical zone.

While its user guidance documents provide adequate advice for securing its operational environment, it is primarily the product administrator's responsibility to ensure that the networks and the systems which the nGenius Service Assurance Solution V4.7 MR2 is connected to or installed on are protected adequately.

8 Architectural Information

The TOE is the set of software components for the nGenius Service Assurance Solution V4.7 MR2, which consists of the following:

- **nGenius InfiniStream.** The InfiniStream application is a continuous capture platform that records the packet-level details of enterprise traffic seen by monitoring network links. The InfiniStream component comprises the following subsystems:

    - *Configuration and administration subsystem* is used for initially configuring the InfiniStream to accept communications from the managing Performance Manager.

    - *NS-Probe subsystem* interacts with the PM-Core subsystem on the Performance Manager to receive, maintain, and enforce policy settings on the InfiniStream.

    - *NS-Network driver subsystem* is a custom network driver that controls the InfiniStream network interface cards.

- **nGenius Performance Manager.** The Performance Manager is a GUI-based management product that is used to control and monitor the operation of one or more

InfiniStream platforms as well as analyze the captured data. The Performance Manager is accessed via a remote workstation over HTTPS and provides user management, security attributes management, user data protection and audit functionality. The Performance Manager comprises the following subsystems:

- *GUI subsystem* presents a java-driven HTML interface to external users using a browser and applet to interact with the TOE for administration and data analysis purposes.
- *PM-core subsystem* provides TOE startup and shutdown functions and the base analysis capabilities of Performance Manager. It also provides communications with any configured InfiniStream devices.
- *Security framework subsystem* enforces the TOE identification and authentication security functions including password authentication, user identification, associating subjects with their assigned role and other attributes.
- *K2 subsystem* is a licensable option that may be purchased by end users and enabled. This subsystem provides specialized data analysis capabilities for specific markets, and plugs into the Performance Manager architecture.

9 Evaluated Configuration

The evaluated configuration consists of the following software:

- nGenius InfiniStream Version 4.70.603;
- nGenius Performance Manager Version 4.70.352; and
- nGenius K2 Version 4.70.352.

The evaluated configuration for the nGenius Service Assuarance Solution V4.7 MR2 has the following attributes:

- Identification and authentication are performed locally by the TOE;
- The Performance Manager / K2 is installed as a Standalone Server;
- SNMPv3 functionality provided by the operational environment is used to provide a channel between Performance Manager / K2 and individual InfiniStream application instances;
- The following optional product components are not installed: nGenius NewsStand for Remote Servers, nGenius Command Line Interface (CLI), nGenius Command Line

Administrator (CLA), nGenius Common Data Export (CDE), Command Line Device Tools, Sniffer Analysis, and Standby Server;

- The serviceManager.userAccountLockup.enabled configuration parameter is set to True to force accounts to be locked out for a specified period of time after the configured number of consecutive authentication failures has occurred;
- The "Change Config Server Address" option in the InfiniStream is set to the IP address of the Managing Performance Manager, forcing authentication to be performed by Performance Manager. Administrators are procedurally prohibited from using the InfiniStream local console except for setting the "Change Config Server Address" option and the access list;
- HTTPS/SSL is activated on the Performance Manager / K2 platform and all connections from remote users to the Performance Manager / K2 use HTTPS. HTTPS/SSL is provided by the operational environment and beyond the boundary of the TOE being evaluated; and
- Access List Security is configured on all InfiniStream application instances to limit the systems that may remotely access the InfiniStream application instances.

10 Documentation

The NetScout Systems documents provided to the consumer are as follows:

- Common Criteria Supplement for nGenius® InfiniStream® (v4.7 MR2, Patch Build 603) and nGenius® Performance Manager (v4.7 MR2, Patch Build 352);
- nGenius InfiniStream Hardware Installation and Administration Guide;
- nGenius Performance Manager Installation Guide; and
- nGenius Performance Manager Online Help version 4.7 MR2.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the nGenius Service Assurance Solution V4.7 MR2, including the following areas:

Development: The evaluators analyzed the nGenius Service Assurance Solution V4.7 MR2 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the nGenius Service Assurance Solution V4.7 MR2 security architecture description and determined that the initialization process is secure and that the security

functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the nGenius Service Assurance Solution V4.7 MR2 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the nGenius Service Assurance Solution V4.7 MR2 configuration management system and associated documentation was performed. The evaluators found that the nGenius Service Assurance V4.7 MR2 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit at NetScout Systems, the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the nGenius Service Assurance Solution V4.7 MR2 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the nGenius Service Assurance Solution V4.7 MR2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by NetScout Systems for nGenius Service Assurance Solution V4.7 MR2. During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of the nGeniusService Assurance Solution V4.7 MR2. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the nGenius Service Assurance Solution V4.7 MR2 in its operational environment.

All these evaluation 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 penetration tests.

12.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis 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 TOE design was complete.

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.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of DOMUS IT Security Laboratory test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests. The evaluator repeated a third of the developer's test to gain assurance of the developer's overall testing effort. The evaluator chose a subset of tests that exercised all of the TOE's security related interfaces;

b. Security Management: The objective of this test is to confirm the security parameters are able to be securely managed by repeating a subset of the developer's tests as well as a number of independent tests that exercised the security management interfaces;

c. User Data Protection: The objective of these tests is to confirm the TOE's ability to protect user data by performing a number of tests against the Role Based Access Control and Slice Size enforcement functions;

d. Audit: The objective of these tests is to ensure that User Access Events Logging requirements have been met by confirming the capture of logs and the presence of event details as specified in the ST; and

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

e. Identification and Authentication: The evaluator confirmed the claimed operation of the identification and authentication function, including tests to demonstrate the correct operation of the configurable lockout feature, configurable timeout period and password complexity enforcement..

12.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Reconnaissance and exploratory testing to observe application behavior including client side script and HTTP packet inspection;
- Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;
- Use of automated SQL injection tools to test login form;
- Capture and analysis of session keys to determine susceptibility to prediction; and
- Penetration attempts involving manipulation of client side variables.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The nGenius Service Assurance Solution V4.7 MR2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at DOMUS IT Security Laboratory. 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 a separate Test Results document.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that nGenius Service Assurance Solution V4.7 MR2 behaves as specified in its ST and functional specification and TOE design.

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 nGenius Service Assurance Solution V4.7 MR2 provides a powerful network service assurance solution supported by desirable security functionality. It is recommended that uses wishing to deploy the evaluated configuration follow the guidance provided in the Common Criteria Supplement.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACL	Access Control List
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CDE	Common Data Export
CLA	Command Line Administrator
CLI	Command Line Interface
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
HTML	Hyper Text Markup Language
HTTPS	Secure Hyper Text Transfer Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MR	Maintenance Release
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. NetScout Systems, Inc. nGenius® InfiniStream® (V4.7 MR2), nGenius® Performance Manager (V4.7 MR2), and nGenius® K2 (V4.7 MR2) Security Target, v14.0, 6 April 2010.

e. NetScout Systems, Inc. Evaluation Technical Report, v1.0, 28 April 2010.