# Certification Report

## EAL 4+ Evaluation of Nortel VPN Router v7.05 and Client Workstation v7.11

Issued by:

**Communications Security Establishment Canada**

**Certification Body**

**Canadian Common Criteria Evaluation and Certification Scheme**



**Document number**: 383-4-69-CR
**Version**: 1.0
**Date**: 27 August 2008
**Pagination**: i to iv, 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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 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 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 EWA-Canada 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) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 20 August 2008, 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/services/common-criteria/trusted-products-e.html and http://www.commoncriteriaportal.org

This certification report makes reference to the following trademarked names:

- Nortel, the Nortel logo and the Globemark are trademarks of Nortel Networks.

# TABLE OF CONTENTS

## Executive Summary

The Nortel VPN Router v7.05 and Client Workstation v7.11 (hereafter referred to as Nortel VPN Router), from Nortel Networks, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 22 July 2008 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

Nortel VPN Router allows users of a private enterprise network to have secure access to that network from a remote location. The Router provides firewall, routing, encryption and decryption, authentication, and data integrity services to ensure that data is securely tunneled across Internet Protocol (IP) networks including the Internet. The Router can also be configured to allow two separate portions of an enterprise network to be securely connected via the Internet. Nortel VPN Router incorporates FIPS 140-2 validated cryptography.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Nortel VPN Router, 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 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.2 – Flaw reporting procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Nortel VPN Router 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[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.

# 1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the Nortel VPN Router v7.05 and Client Workstation v7.11 (hereafter referred to as Nortel VPN Router), from Nortel Networks.

# 2 TOE Description

Nortel VPN Router allows users of a private enterprise network to have secure access to that network from a remote location. The Router provides firewall, routing, encryption and decryption, authentication, and data integrity services to ensure that data is securely tunneled across Internet Protocol (IP) networks including the Internet. The Router can also be configured to allow two separate portions of an enterprise network to be securely connected via the Internet.

Nortel VPN Router provides stateful inspection firewall functionality which protects the private enterprise network from attack by parties on the Internet. The firewall inspects the packets flowing through the router and uses administrator-configurable rules to determine whether or not to allow each packet to pass through to its intended destination.

Nortel VPN Router has been evaluated on the hardware appliance models 600, 1010, 1050, 1100, 1750, 2750, and 5000. These models provide identical functionality and differ only in throughput and performance.

# 3 Evaluated Security Functionality

The complete list of evaluated security functionality for Nortel VPN Router is identified in Section 5 of the Security Target (ST).

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

| **Cryptographic Module** | **Certificate #** |
|---|---|
| VPN Router 1750, 2700, 2750 and 5000 with Hardware Accelerator | *Pending* [2] |
| VPN Router 1750, 2700, 2750 and 5000 with VPN Router Security Accelerator | *Pending* |
| Nortel VPN Router 600, 1750, 2700, 2750 and 5000 | *Pending* |
| Nortel VPN Router 1010, 1050 and 1100 | *Pending* |
| VPN Client Software | *Pending* |

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Nortel VPN Router:

| **Cryptographic Algorithm** | **Standard** | **Certificate #** |
|---|---|---|
| Triple-DES (3DES) | FIPS 46-3 | 641, 642, 644 |
| Advanced Encryption Standard (AES) | FIPS 197 | 718, 719, 721 |
| Rivest Shamir Adleman (RSA) | FIPS 186-2 | 338, 339 |
| Secure Hash Algorithm (SHA-1) | FIPS 180-2 | 738, 739, 740 |
| Keyed-Hash Message Authentication Code (HMAC) | FIPS 198 | 387, 388, 389 |

# 4 Security Target

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

Title: Nortel Networks VPN Router v7.05 and Client Workstation v7.11 Security Target
Version: Version 3.8
Date: 18 March 2008

# 5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

Nortel VPN Router 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 4 augmented, containing all the security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 Flaw reporting procedures.

# 6 Security Policy

Nortel VPN Router implements the following Security Policies:

- Access Control, that controls administrator access to configuration parameters;
- VPN Information Flow Control, that controls encrypted information flow; and
- Firewall Information Flow Control, that controls firewall information flow.

In addition, Nortel VPN Router implements security policies pertaining to security audit, cryptographic support, identification and authentication, security management, protection of

TOE security functions, and trusted path/channels. Further details on these security policies are found in Section 5 of the ST.

# 7 Assumptions and Clarification of Scope

Consumers of Nortel VPN Router 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 Nortel VPN Router.

## 7.1 Secure Usage Assumptions

The following Secure Usage assumptions are listed in the ST:

- It is assumed that administrators will be trained in the secure use of the TOE and will follow the policies and procedures defined in the TOE documentation for secure administration of the TOE. Administrators are assumed to be non-hostile.

## 7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- It is assumed that the TOE relies on the operating environment of TOE to provide accurate clock time in order to create an accurate time stamp for audit events.
- It is assumed that the TOE will be housed within a physically secure environment.
- It is assumed that the environment will provide the necessary infrastructure to ensure that certificates can be validated when digital certificates are used for authentication. It is assumed that the appropriate infrastructure is properly maintained in order to ensure the accuracy and security of the certificates (e.g., certificates are revoked in a timely manner).
- It is assumed that the TOE has access to all of the Information Technology (IT) System data it needs to perform its functions.

## 7.3 Clarification of Scope

The TOE is intended for use by non-hostile and well trained network administrators that have followed the installation and configuration guidance provided in: Nortel Networks Virtual Private Network Router v7.05 Supplement Guide; and Nortel VPN Router Configuration – FIPS 140-2.

# 8 Architectural Information

Nortel VPN Router comprises the Router component and the Client component.

The Router component is firmware that runs on the purpose built FIPS 140-2 validated hardware appliance models 600, 1010, 1050, 1100, 1750, 2750, and 5000. The Router comprises the subsystems:

- Administrator interface;
- Database;
- Control;
- Context; and
- Servicing.

The Client component is software that runs on a remote user's general purpose workstation. The Client comprises the subsystems:

- VPN Interface;
- User Interface; and
- VPN Client.

Further details about the Nortel VPN Router architecture are proprietary to the vendor, and are not provided in this report.

# 9 Evaluated Configuration

The ST defines the Router component as Nortel VPN Router v7.05 build 100 that runs on the FIPS 140-2 validated hardware appliance models 600, 1010, 1050, 1100, 1750, 2750, and 5000. The Client component is defined as Nortel VPN Client Workstation v7.11 build 100 that runs on Microsoft Windows 2000 SP4 and XP SP2 (32 bit).

Nortel VPN Router must be running in FIPS mode. This is specified in the Nortel Networks Virtual Private Network Router v7.05 Supplement Guide.

# 10 Documentation

The significant Nortel Networks documents provided to the consumer are as follows:

a. Nortel VPN Router Installation;
b. Nortel VPN Router Configuration – FIPS 140-2;
c. Using Contivity Secure IP Services Gateways in FIPS mode;
d. Nortel Networks Virtual Private Network Router v7.05 Supplement Guide;
e. Nortel VPN Router Configuration – Firewalls, Filters, NAT, and QoS;
f. Nortel VPN Router Configuration – Tunneling Protocols;
g. Configuring Basic Features for the Contivity Secure IP Services Gateway; and
h. Configuring Advanced Features for the Contivity Secure IP Services Gateway.

# 11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Nortel VPN Router, including the following areas:

**Configuration management:** An analysis of the Nortel VPN Router configuration management system and associated documentation was performed. The evaluators found that

Nortel VPN Router configuration items were clearly marked, and could be modified and controlled. 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 Nortel VPN Router 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 Nortel VPN Router functional specification, high-level design, low-level design, security policy model, and a subset of the implementation representation; they determined that the documents were internally consistent, and completely and accurately instantiated 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 Nortel VPN Router 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 examined 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 Nortel VPN Router design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Nortel Networks for the Nortel VPN Router. During a site visit, the evaluators also 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 Nortel VPN Router ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for Nortel VPN Router and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

# 12 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

## 12.1 Assessing 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[3].

Nortel Networks employs a rigorous testing process that tests the changes and fixes in each release of Nortel VPN Router. Comprehensive regression testing is conducted for a General Availability targeted release.

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification 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 EWA-Canada test goals:

a. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;
b. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
c. Firewall: The objective of this test goal is to ensure that the network segregation, flow control, and protection requirements have been met with the Firewall functionality;
d. Data Protection: The objective of this test goal is to determine the TOE's VPN capability for protecting its data; and
e. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

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

### 12.3 Independent Penetration Testing

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

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

Vulnerability sites were searched for vulnerabilities. Testing included scanning for generic weaknesses, monitoring network traffic during start up and operation for information leakage and carrying out basic protocol attacks.

The independent penetration testing, and subsequent ad-hoc testing, did not uncover any exploitable vulnerabilities in the anticipated operating environment.

### 12.4 Conduct of Testing

Nortel VPN Router 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 EWA-Canada. 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 Nortel VPN Router behaves as specified in its ST and functional specification.

## 13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ 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 complete documentation for Nortel VPN Router includes a comprehensive Installation, Configuration and Security Guide.

The Nortel VPN Router is straightforward to configure, use and integrate into a corporate network. The Web GUI is intuitive and provides the administrator with a one stop tool for management.

Nortel Networks Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

EWA-Canada performed a site visit to review the developer's processes, product life-cycle and site security, and to repeat a sample of the developer's tests. The evaluator found the company was well established and practising sound and documented processes in order to develop their products. Nortel Networks demonstrated a strong commitment to the Common Criteria evaluation and its completion.

# 15 Acronyms, Abbreviations and Initializations

| Acronym/Abbreviation/ Initialization | Description |
|---|---|
| 3DES | Triple - Data Encryption Standard |
| AES | Advanced Encryption Standard |
| CC | Common Criteria |
| CCEF | Common Criteria Evaluation Facility |
| CCS | Canadian Common Criteria Evaluation and Certification Scheme |
| CPL | Certified Products list |
| CM | Configuration Management |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| FIPS | Federal Information Processing Standard |
| GUI | Graphical User Interface |
| HMAC | Hashed Message Authentication Code |
| IP | Internet Protocol |
| IPSec | IP Security |
| IT | Information Technology |
| ITSET | Information Technology Security Evaluation and Testing |
| OS | Operating System |
| PALCAN | Program for the Accreditation of Laboratories Canada |
| QA | Quality Assurance |
| RSA | The algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT; the letters **RSA** are the initials of their surnames. |
| SANS | SysAdmin, Audit, Network, Security |
| SFP | Security Function Policy |
| SHA-1 | Secure Hash Algorithm |

| Acronym/Abbreviation/ Initialization | Description |
|---|---|
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Function |
| US-CERT | United States Computer Emergency Readiness Team |
| VPN | Virtual Private Network |

# 16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.
b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.
c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.
d. Nortel Networks VPN Router v7.05 and Client Workstation v7.11 Security Target, Version 3.8, 18 March 2008.
e. Evaluation Technical Report for Common Criteria EAL 4+ Evaluation of Nortel VPN Router v7.05 and Client Workstation v7.11 Document No. 1548-000-D002, Version 1.4, 22 July 2008.