Certification Report

EAL 4 Evaluation of

Nortel Networks Alteon Switched Firewall (Version 2.0.3 with Hotfix 315/NG_FP3_HFA_315)

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-31
Version: 1.0
Date: 10 June 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 Revision 256*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.2 Revision 256*. 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 10 June 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 Alteon, Alteon Switched Firewall, ASF 5308, ASF 5408, ASF 5610, ASF 5710, Firewall Operating Ssystem, Firewall Director, SFD 5008, SFD 5010, Accelerator Operating System, Firewall Accelerator, SFA 5300, SFA 5400, SFA 5600 and SFA 5700 which are trademarks of Nortel Networks Inc. in the United States and certain other countries. FireWall-1 NG is a registered trademark of Check Point Software Technologies.

TABLE OF CONTENTS

Executive Summary

The Nortel Networks Alteon Switched Firewall (Version 2.0.3 with Hotfix 315/NG_FP3_HFA_315); hereafter referred to as the Alteon Switched Firewall Version 2.0.3, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation.

The Alteon Switched Firewall Version 2.0.3 is a high-performance firewall system for network security. The system uses a versatile, multi-component approach to deliver accelerated firewall processing power. A basic system is composed of a Switched Firewall Director (SFD) and a Switched Firewall Accelerator (SFA). The SFD, which is comprised of the Firewall Operating System and the Check Point FireWall-1 FP3, handles firewall policies and inspects network traffic. The SFA offloads the processing of secured traffic and speeds up firewall performance. The Alteon Switched Firewall Version 2.0.3 is designed to be installed and operated in an environment that is configured and controlled in accordance with the 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 3 June 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 Alteon Switched Firewall Version 2.0.3, the security requirements, and the level of confidence (evaluation assurance level) to which the product is intended to satisfy the security requirements. Consumers of the Alteon Switched Firewall Version 2.0.3 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 4 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 Revision 256* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.2 Revision 256*.

The Communications Security Establishment, as the CCS Certification Body, declares that the Alteon Switched Firewall Version 2.0.3 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 Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is the Nortel Networks Alteon Switched Firewall (Version 2.0.3 with Hotfix 315/NG_FP3_HFA_315); hereafter referred to as the Alteon Switched Firewall Version 2.0.3.

2 TOE Description

The Alteon Switched Firewall Version 2.0.3 is a high-performance firewall system for network security. The system uses a versatile, multi-component approach to deliver accelerated firewall processing power.

A basic system is composed of a Switched Firewall Director (SFD) and a Switched Firewall Accelerator (SFA). The SFD consist of an Alteon 5010 or 5008 running the Firewall Operating System and the Check Point FireWall-1 NG FP3 software which inspects network traffic and handles firewall policies. The SFA consists of an Alteon 5700, 5600, 5400 or 5300 switch running the Accelerator Operating System software which offloads the processing of secured traffic and speeds up firewall performance.

The Check Point FireWall-1 Module is a stateful inspection firewall which supervises the traffic passing between networks physically connected to the TOE and belonging to the complete 'IP' family of protocols. Supervision is based on the information contained in protocol headers and the product's computer system, including state information derived from one or more associated packets.

The Check Point FireWall-1 Module is also the component of the Alteon Switched Firewall Version 2.0.3 which performs policy checking for every new connection request, manages the connection table and specifies the rules for handling subsequent packets in a session. Once a session is active, the policy checking for packets is handled by the SFA. In this way, once the SFD inspection engine accepts the setup packets in a session, subsequent packets belonging to the session are inspected by the SFA without the involvement of the SFD.

The TOE is configured and administered by means of a remote connection to the Check Point VPN-1/FireWall-1 NG Management Server and management GUI. This connection is protected by encryption.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Alteon Switched Firewall Version 2.0.3 is identified in Section 5 of the Security Target.

4 Security Target

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

Title: Common Criteria EAL4 Evaluation, Nortel Networks, Alteon Switched Firewall (Version 2.0.3 with Hotfix 315/NG_FP3_HFA_315)
Version: 1.5
Date: 3 June 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.2 Revision 256*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.2 Revision 256*, incorporating all final interpretations issued prior to 7 June 2004.

The Alteon Switched Firewall Version 2.0.3 is:

a. Common Criteria Part 2 extended, with security functional requirements based 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 conformant, with all the security assurance requirements in the EAL 4 package.

6 Security Policies

The Alteon Switched Firewall Version 2.0.3 Security Policies are identified in the ST. The following statements are representative of the Security Policies.

6.1 Network Traffic Flow Control

Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if:

a. all of the information security attribute values are unambiguously permitted by the information flow control security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by the authorized administrator; and

b. the presumed address of the destination subject, in the information, translates to an address on some other connected network.

6.2 Secure Internal Communications Flow Control

Secure use of the TOE requires a secure internal communications channel between the TOE and the Check Point Management Server. The TOE imposes a requirement on its IT environment to provide this secure internal communications channel. This requirement is met via an implementation of the standard TLS protocol defined in RFC 2246. To meet the requirement, the IT environment shall permit an information flow between the TOE and the Check Point Management Server if based on the X.509 certificates installed upon these components, a trusted connection can be negotiated via the TLS protocol.

6.3 Virtual Private Network

The TOE supports Virtual Private Network (VPN) connections between the TOE and VPN enabled clients. The TOE imposes upon its IT environment a requirement for cryptographic functionality to support the VPN connection. The requirement is met via an implementation of the standard IPSec protocol. To meet the requirement, the IT environment shall permit an information flow between the TOE and a VPN enabled client if an encrypted connection can be established via the IPSec protocols.

7 Assumptions and Clarification of Scope

Consumers of the Alteon Switched Firewall Version 2.0.3 product 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

It is assumed that the product is installed, configured, operated and maintained in accordance with the procedures and guidelines defined in the Installation and User Guide and other associated documents for the Alteon Switched Firewall Version 2.0.3.

It is further assumed that:

a. the product is configured with the minimum of operating system features installed and the minimum of operating system features enabled to permit operation of the product;

b. computer system privileges as assigned to programs in accordance with the site security policy;

c. physical security controls prevent unauthorized access to the product, management server, consoles and system devices;

d. the product is configured with user accounts for authorized administrators only;

e. the administrators' use of privileged accounts conforms to the site security policy;

f. restrictions imposed by site security policies concerning the choice of system passwords are enforced by the computer system configuration;

g. guidelines consistent with the site security policy are followed for operating system controlled ownership and restrictions on access to operating system and product directories and files;

h. computer system backup and recovery procedures are followed which are sufficient to restore the product to a secure state after a failure of the product;

i. appropriate use is made of the management server's facilities to examine the audit log file and ensure that the size of the log file does not exceed the file system size limits;

j. the firewall security policy will be configured to deny all network connections aimed directly at the firewall host, except from the management server; and

k. administrators have knowledge of the product, the Linux operating system and networking technologies.

7.2 Environmental Assumptions

It is assumed that the computer system hosting elements of the TOE along with any associated devices function correctly.

It is assumed that the product is operated in a 'trusted configuration' as defined in the Security Target.

It is assumed that the product is adequately protected against physical threats.

7.3 Clarification of Scope

The Alteon Switched Firewall Version 2.0.3 can not prevent authorized administrators from carelessly configuring the Firewall such that the information flow control policy is compromised.

8 Architectural Information

An Alteon Switched Firewall Version 2.0.3 consists of two hardware units and the software associated with these units. The two hardware units are the Switched Firewall Director (SFD) and the Switched Firewall Accelerator (SFA). The SFD runs the Check Point FireWall-1/VPN-1 NG FP3 firewall software on top of a Linux operating system. The SFA

unit runs the Accelerator Operating System software which is responsible for offloading the processing of secured traffic.

9 Evaluated Configuration

The evaluated configurations of the TOE are:

- The 5308 model of the Alteon Switched Firewall Version 2.0.3 which consists of a 5300 SFA component and a 5008 SFD component.
- The 5408 model of the Alteon Switched Firewall Version 2.0.3 which consists of a 5400 SFA component and a 5008 SFD component.
- The 5610 model of the Alteon Switched Firewall Version 2.0.3 which consists of a 5600 SFA component and a 5010 SFD component.
- The 5710 model of the Alteon Switched Firewall Version 2.0.3 which consists of a 5700 SFA component and a 5010 SFD component.

10 Documentation

a. Installation and User's Guide, Alteon Switched Firewall, Release 2.0.3, Part Number 212535-C, October 2002.

b. Release Notes, Alteon Switched Firewall, Release 2.0.3, Part Number 213028-E, November 2002.

c. Common Criteria Certified Software, Appendix E, Part Number 215709-B, June 2004.

11 Evaluation Analysis Activities

In all areas of the evaluation except for the vulnerability assessment, the evaluators considered the results of a previous evaluation of the TOE (see reference D and E) and where appropriate reused evidence from the previous evaluation. However to ensure that the current evaluation considered up-to-date vulnerability information, the vulnerability analysis work units were repeated completely without any reuse of results from the previous evaluation.

The evaluation analysis activities involved a structured evaluation of the Alteon Switched Firewall Version 2.0.3, including the following areas:

Configuration management: The evaluators performed an analysis of the Alteon Switched Firewall Version 2.0.3 development environment and associated documentation. The evaluators determined that the configuration items which comprise the TOE are clearly

identified and labelled and that control is exercised over all modifications to the configuration items. The analysis was supplemented by a site visit to the development offices of Check Point Software Limited who are the developers of the VPN-1/Firewall-1 software which provides the majority of the security functionality for the TOE. The site visit confirmed that the configuration control procedures in place at Check Point are mature and stable.

Secure delivery and operation: The evaluators examined the delivery documentation for the Alteon Switched Firewall Version 2.0.3 product and determined that it is adequate to maintain the integrity of the TOE during delivery to the consumer. The evaluators examined and tested the installation, generation and start-up procedures for the TOE and determined that they are complete and sufficiently detailed and result in a secure installation of the TOE.

Design documentation: The evaluators reviewed the design documentation for the Alteon Switched Firewall Version 2.0.3 including the functional specification, high-level design, low level design, security policy model and source code. In addition, the evaluators made a site visit to the Check Point development facility in Israel to review the source code for the Check Point modules used with the Alteon Switched Firewall Version 2.0.3 product. The evaluators concluded that the design documents completely and accurately describe all interfaces and security functions of the product and are internally consistent.

Guidance documents: The evaluators reviewed the Alteon Switched Firewall Version 2.0.3 guidance documents and determined that they clearly and unambiguously describe how to securely use and administer the product and that they are consistent with the other documents supplied for the evaluation.

Life-cycle support: The evaluator reviewed the life cycle support documentation for the TOE. The evaluator concluded that the developers have used well-defined development tools which yield consistent and predictable results. The evaluators also determined that the developers have used a well defined and documented life cycle model for the TOE. The evaluators also concluded that the development security measures applied by the developers provide sufficient assurance of the confidentiality and integrity of the TOE. These conclusions apply equally to Nortel, the primary developers of the TOE and Check Point, who are the developers of the firewall software which provides the majority of the security functionality of the TOE.

Vulnerability assessment: The evaluator's reviewed the developers vulnerability analysis and performed and independent vulnerability analysis to develop penetration tests for the TOE. Refer to the next section of the report for additional details of the vulnerability testing.

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

12 ITS Product Testing

The evaluators reviewed the testing evidence produced by the developers and the independent testing conducted during the previous evaluation of the TOE. In addition, the evaluators carried out independent vulnerability testing of the TOE.

12.1 Assessing Developer Tests

The evaluators confirmed that the developer met their testing responsibilities for the TOE by examining the developer test evidence and reviewing the developer test results as well as examining the results of independent testing conducted during a previous evaluation of the TOE.

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

12.2 Previous Evaluation Testing

Extensive independent functional and penetration testing was completed during a previous evaluation of the product (refer to References D and E). The evaluators for the current evaluation reviewed the results of this testing and concluded that the testing conducted during the original evaluation was thorough and rigorous. Therefore the test results from the previous evaluation have been reused for the current evaluation.

12.3 Independent Vulnerability Testing

After reviewing the developers test and vulnerability analysis evidence, the evaluators employed a flaw hypothesis methodology to develop a list of potentially exploitable vulnerabilities of the TOE in the following areas:

a. Generic vulnerabilities;

b. Bypassing;

c. Tampering;

d. Direct attacks; and

e. Misuse.

Test cases were then developed, documented and executed in an attempt to exploit the postulated vulnerabilities. Extensive use was made of public domain network attack tools in

an attempt to compromise the TOE. The independent penetration testing did not uncover any new vulnerabilities in the TOE.

12.4 Conduct of Testing

The TOE was installed and configured in the IT Security Evaluation and Testing (ITSET) facility at Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario. All penetration and vulnerability testing was conducted at this facility. The CCS Certification Body witnessed a portion of the testing.

12.5 Test Results

All independent penetration tests and vulnerability tests yielded the expected results. The previously evaluated version of the TOE was found to be vulnerable to a well known HTTP Security Server attack which is easily available in the public domain. This vulnerability was first exposed after the original evaluation of the TOE. The developer has issued an update to the product which eliminates the vulnerability. The evaluators tested the TOE in its original configuration to confirm the existence of the vulnerability, and subsequently tested the updated version of the TOE to confirm that the vulnerability had been removed from the TOE. No additional exploitable vulnerabilities were uncovered during the testing.

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 independent vulnerability analysis conducted during this evaluation revealed a single known vulnerability in the HTTP Security Server module of the Check Point VPN-1/Firewall-1 Module. This vulnerability has been eliminated by Check Point and Nortel through the issue of an update to the Check Point software.

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
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
VPN	Virtual Private Network

16 References

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

a) Common Criteria for Information Technology Security Evaluation, Parts 1-3, January 2004, Version 2.2 Revision 256 (CCIMB-2004-01-001/002/003).

b) Common Methodology for Information Technology Security Evaluation, CCIMB-2004-01-004, Part 2: Evaluation and Methodology, Version 2.2 Revision 256, January 2004 (CCIMB-2004-01-004).

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

d) Common Criteria Certification Report No. P189, Nortel Networks Alteon Switched Firewall, version 2.0.3.0 running of specified platforms, Issue 1.0, August 2003.

e) Task LFD/T320 Evaluation Technical Report, Issue 1.0, Doc Ref: P19851/Eval/R-02/01, April 2003.

f) Common Criteria EAL 4 Evaluation, Nortel Networks, Alteon Switched Firewall (Version 2.0.3.0), Security Target 1.3, 5 October 2004.

g) Evaluation Technical Report (ETR), Nortel Networks Alteon Switched Firewall, EAL Evaluation, Common Criteria Evaluation Number, 383-4-31, Document No. 1480-000-D002, Version 1.0, 24 May 2005.