Certification Report

EAL 4 Evaluation of

WatchGuard Technologies, Inc.

Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number:	383-4-30
Version:	1.0
Date:	30 June 2005
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 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.1*. 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) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 8 July 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 WatchGuard and Firebox which are trademarks or registered trademarks of WatchGuard Technologies, Inc.

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

TABLE OF CONTENTS

Executive Summary

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0.[1]

The Firebox® X Family of firewalls are traffic-filter firewalls that filter traffic based on policies set by the system administrator. The administrator can set policies based on source address of the information, destination address of the information, what service the traffic is using (HTTP, HTTPS, FTP, etc.), the source port of the information, the destination port of the information, and the interface the traffic arrives or exits on (Internal/External).

Electronic Warfare Associates-Canada, Ltd. is the CCEF that conducted the evaluation. This evaluation was completed on 30 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0, 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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[2] 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 1.0* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*.

The Communications Security Establishment, as the CCS Certification Body, declares that the WatchGuard Technologies, Inc. Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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 Core™ Series comprises models X500, X700, X1000, and X2500; the Peak™ Series comprises models X5000, X6000, and X8000.

[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.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 evaluation is the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0, from WatchGuard Technologies, Inc.

2 TOE Description

The TOE comprises the Firebox® X Family: Core™ Series X500, X700, X1000, and X2500 and the Peak™ Series X5000, X6000, and X8000.

All of the Firebox® X Family appliances employ a hardened Linux operating system that is based on Kernel version 2.4. Linux processes not essential to the Firebox® X Family have been removed. There is no method of accessing the operating system directly.

The Firebox® X Family of firewalls filter traffic coming through the appliance based on policies that are created by the system administrator. In the Common Criteria Mode of operation, the administrator can add policies based on: source address of the information, destination address of the information, what service the traffic is using (HTTP, HTTPS, FTP, etc.), the source port of the information, the destination port of the information, and the interface the traffic arrives or exits on (Internal/External).

The only method of administering the Firebox® X Family is through the command line interface (CLI).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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:	WatchGuard Technologies, Inc. Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 Security Target
Version:	2.1
Date:	June 27, 2005

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 1.0*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.1*, incorporating all final interpretations issued prior to May 2004.

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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.

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 conforms with the *U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (TFFPP).*

6 Security Policy

The Firebox® X Family implements an information flow control policy. The subjects under the control of this policy are external IT entities sending information through the TOE to internal IT entities, and internal IT entities sending information through the TOE to external IT entities. Policy detail can be found in the Section 5.1.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 is designed for use by network administrators and it is assumed that these administrators are appropriately trained and experienced and have no malicious intentions.

It assumed that the product will be installed and configured using the guidance documents provided by WatchGuard Technologies, Inc. These documents are listed in Section 10.

7.2 Environmental Assumptions

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 is designed to control the flow of information between networks. For these appliances to be effective it is assumed that information may not flow between the networks without passing through the TOE.

The only CC approved method of Firebox® administration is through a command line interface (CLI) that resides in the same physically secure location as the TOE. The device can be managed only with this direct serial connection. Remote management is not supported in Common Criteria mode. All policies that allow remote management are disabled. It is further assumed that access to the console is restricted to authorized administrators.

7.3 Clarification of Scope

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 can not prevent authorized administrators from carelessly configuring a Firewall such that the information flow control policy is compromised.

8 Architectural Information

The Firebox® X Family of firewalls comprise a hardware platform, a hardened Linux operating system that is based on Kernel version 2.4, and Fireware™ Version 8.0.

The Firebox® X Family implements an information flow control policy. Policy enforcement is performed by the Fireware™ Version 8.0 RapidCore software application. The RapidCore application handles all information flow and the storeage of user account information, audit records, and policy information.

For additional architectural information refer to Section 2 of the ST.

9 Evaluated Configuration

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 evaluated configuration comprises:

- the Core™ Series hardware configuration models: X500, X700, X1000, X2500, and
- the Peak™ Series hardware configuration models: X5000, X6000, X8000.

The firmware version for all Firebox® X Family models is Fireware™ Version 8.0, build 4057.

In the evaluated configuration, a CC Mode is enabled in accordance with Chapter 5 of the publication entitled WatchGuard® Fireware Command Line Interface (WatchGuard Fireware v8.0). The evaluated configuration is limited to administration through the CLI only and does not include Virtual Private Network (VPN), Demilitarized Zone (DMZ), or High Availability (HA) functionality.

10 Documentation

The following publications describe all the procedures necessary to install and operate the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 in its evaluated configuration (CC mode):

- WatchGuard Technologies, Inc. Operating the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 in Common Criteria Operation Mode, Document Version 1.0.
- WatchGuard Technologies, Inc. Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 Command Line Interface Reference, Document Version 1.0.

WatchGuard Technologies, Inc. also provides additional hardware, configuration, upgrade, reference and user guides for the WatchGuard® System Manager (WSM) - one version for the 500, 700, 1000 and 2500 and another for the 5000, 6000 and 8000 [3].

[3] *The Fireware Command Line Interface v8.0 (CLI) and the WatchGuard® System Manager (WSM) user interface v8.0 are not designed to be used together. The CLI and WSM interface do not create compatible configuration files. The CLI is only for use in Common Criteria mode. When you enable Common Criteria mode, the CLI disables the ability to create and edit a configuration file with the WSM software. While in Common Criteria mode, you must use the CLI to make all configuration changes.*

Core™ Series Documentation:

- WatchGuard® System Manager User Guide, Doc Version: 8.0-050411
- WatchGuard® System Manager Reference Guide, Doc Version: 8.0-050410
- WatchGuard System Manager 7.x to 8.0 Upgrade Instructions (pamphlet)
- WatchGuard® System Manager Fireware Configuration Guide, Doc Version: 8.0-050411
- WatchGuard® System Manager WFS Configuration Guide, Doc Version: 7.4-050411
- Firebox X Hardware Guide, Part No: 1311-001
- WatchGuard® Fireware™ Pro Migration Guide , Doc Version: 8.0-050420
- WatchGuard® Mobile User VPN Administration Guide, Doc Version: 8.0-050411
- WatchGuard® Mobile User VPN Client End User Brochure – Windows 2000, Version: 6.0, Part No: 1200016
- WatchGuard® Mobile User VPN Client End User Brochure-Windows NT, Version 6.0, Part No: 1200016
- WatchGuard® Mobile User VPN Client End User Brochure-Windows XP, Version 6.0, Part No: 1200016

Peak™ Series Documentation:

- WatchGuard® System Manager User Guide, Doc Version: 8.0-050411
- WatchGuard® System Manager Reference Guide, Doc Version: Reference-8.0-050410
- WatchGuard® System Manager Fireware Configuration Guide, Guide Version: 8.0-050411
- Firebox® X Peak Hardware Guide, Doc Version: 8.0, Publication ID: 1311-001, Text ID: 1311-000
- WatchGuard® Firebox X Peak™ QuickStart Guide, Part No. 2065-002 WGCX66239_0405
- WatchGuard® Fireware™ Pro Migration Guide, Guide Version: 8.0-050420

- WatchGuard® Mobile User VPN Administrator Guide, Document Version: 8.0-050411

- WatchGuard® Mobile User VPN Client End User Brochure – Windows 2000, Version 6.0, Part No: 1200016

- WatchGuard® Mobile User VPN Client End User Brochure-Windows NT, Version 6.0, Part No: 1200016

- WatchGuard® Mobile User VPN Client End User Brochure-Windows XP, Version 6.0, Part No: 1200016

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0, including the following areas:

Configuration management: An analysis of the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 development environment and associated documentation was performed. The evaluators found that the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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 two site visits, 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 functional specification, high-level design, low level design, security policy model and source code. 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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 two site visits and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 design and implementation. The evaluators determined that the developer has used a documented model of the product life cycle. The evaluators determined that the developer has used well-defined development tools that yield consistent and predictable results.

Vulnerability assessment: The strength of function claims made in the Security Target for the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 were validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability, misuse and strength of function analyses. In addition, the evaluators performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0.

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

12 ITS Product Testing

Testing at EAL 4 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 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 was complete.

Based on a review of the developer's tests, independent testing concentrated on the following areas:

a. audit;
b. identification and authentication;
c. information flow control; and
d. security management

Tests were selected which demonstrate that the TOE satisfies the security functional requirements specified in the Security Target. A total of seven (7) individual tests were selected for the evaluation, representing approximately 27% of the developer's test cases that are applicable to the evaluated configuration.

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

After reviewing the technical specifications and product documentation, a flaw hypothesis methodology was used to develop a list of potential vulnerabilities of the TOE. Those 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.

A total of 32 penetration attacks were developed and exercised against the TOE.

Penetration testing did not uncover any exploitable vulnerabilities for the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 in its anticipated operating environment.

12.4 Conduct of Testing

The Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 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[4].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 behaves as specified in the 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 Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 includes comprehensive guides for the installation, configuration and operation of the product.

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
CPU	Central Processing Unit
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level

[4] 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.

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
TFFPP	U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999
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, CCIMB-99-031/032/033, Version 2.1, August 1999, annotated with final interpretations issued as of May 2004.

b) Common Methodology for Information Technology Security Evaluation, CEM-99/045, Part 2: Evaluation and Methodology, Version 1.0, August 1999, annotated with final interpretations issued as of May 2004.

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

d) U.S. Government Traffic-Filter Firewall Protection Profile for Low-Risk Environments, Version 1.1, April 1999 (TFFPP).

e) WatchGuard Technologies, Inc. Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0 Security Target, Version 2.1, June 29, 2005.

f) Evaluation Technical Report (ETR), Firebox® X Family: Core™ and Peak™ Series with Fireware™ Version 8.0, Version 1.2, 30 June 2005 [5].

[5] 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