Certification Report

EAL 4+ Evaluation of WatchGuard XTM Firewalls and Fireware XTM Operating System v11.5.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-160-CR
Version: 1.0
Date: 4 May 2012
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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 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 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 EWA-Canada 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 May 2012, 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 (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following registered trademark:

- WatchGuard is a registered trademark of WatchGuard Technologies, Inc. in the United States and/or other countries.

TABLE OF CONTENTS

Executive Summary

WatchGuard XTM Firewalls and Fireware XTM Operating System v11.5.1 (hereafter referred to as XTM Firewalls), from WatchGuard Technologies, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

XTM Firewalls comprises several series of firewall appliances[1] that reside between the network they are protecting and an external network such as the Internet. XTM Firewalls incorporates packet filtering and application proxy techniques to inspect, control, and protect the flow of network traffic that travels in and out of an organization's internal network. XTM Firewalls supports secure remote administration using FIPS 140-2 validated cryptography.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 24 April 2012 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 XTM Firewalls, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its 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)[2] 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 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.* The following augmentation is claimed: ALC_FLR.2 – Basic Flaw Reporting Procedures.

XTM Firewalls is conformant with the *U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1, July 2007* and the *U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1, July 2007.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the XTM Firewalls 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

[1] XTM 2 Series, XTM 5 Series, XTM 8 Series, XTM 1050, and XTM 2050.

[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.

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) 4 augmented evaluation is WatchGuard XTM Firewalls and Fireware XTM Operating System v11.5.1 (hereafter referred to as XTM Firewalls), from WatchGuard Technologies, Inc.

2 TOE Description

XTM Firewalls comprises a series[3] of firewall appliances that reside between the network they are protecting and an external network such as the Internet. XTM Firewalls incorporates packet filtering[4] and application proxy techniques[5] to inspect, control, and protect the flow of network traffic that travels in and out of an organization's internal networks. XTM Firewalls supports secure remote administration using FIPS 140-2 validated cryptography.

A detailed description of the XTM Firewalls architecture is found in Section 1.4 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for XTM Firewalls is identified in Section 6 of the ST.

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

Cryptographic Module	**Part Number**	**Certificate #**
XTM Cryptographic Processor XTM 3	P1020NSE	*Pending* [6]
XTM Cryptographic Processor XTM 2	P1011NSE	*Pending*
XTM Cryptographic Processor XTM 330	P2020NSE	*Pending*
XTM Cryptographic Module Version 11.5.1	Firmware	*Pending*
XTM Cryptographic Processor XTM 8, XTM 1050, and XTM 2050	400BG233-P-G	*Pending*

[3] XTM 2 Series, XTM 5 Series, XTM 8 Series, XTM 1050, and XTM 2050.

[4] Traffic Filter Firewall.

[5] Application-level Firewall.

[6] 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.

Cryptographic Module	Part Number	Certificate #
XTM Cryptographic Processor XTM 5	350BG233-G	*Pending*
XTM Cryptographic Processor XTM 2	NHIXP435AE	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in XTM Firewalls:

Cryptographic Algorithm	Standard	Certificate #
Triple-DES (3DES)	FIPS 46-3	1182, 1181, 1180, 1082, 1080, 1079, 1078
Advanced Encryption Standard (AES)	FIPS 197	1829, 1828, 1827, 1662, 1660, 1659, 1658
Keyed-Hash Message Authentication Code (HMAC) with Secure Hash Algorithm (SHA-1)	FIPS 198	1083, 198, 977, 975, 974, 973

4 Security Target

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

Title: WatchGuard Technologies, Inc. XTM Firewalls and Fireware XTM Operating System v11.5.1 Security Target
Version: 0.8
Date: 13 April 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

XTM Firewalls 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 security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 - Flaw reporting procedures.
d. XTM Firewalls is conformant with the *U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1 July 2007* and the *U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1 July 2007*.

6 Security Policies

XTM Firewalls implement pre-configured packet filter policies and application proxy policies. The administrator can use these pre-configured policies, or modify them to suit the needs of the network environment. The administrator can also create a custom policy based on the following criteria:

- The source address of the information;
- The destination address of the information;
- The service the traffic is using;
- The source port of the information;
- The destination port of the information; and
- The interface the traffic arrives or exits on.

In addition, XTM Firewalls implement policies pertaining to Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, and Protection of the TOE Security Functionality (TSF). Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of XTM Firewalls 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 Assumption is listed in the ST:

- Authorized administrators are non-hostile and follow all administrator guidance, however, they are capable of error.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is physically secure;
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) or storage repository capabilities on the TOE; and

- Information cannot flow between the internal and external networks unless it passes through the TOE.

7.3 Clarification of Scope

XTM Firewalls offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. XTM Firewalls is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

XTM Firewalls comprises a series of firewall appliances. The evaluated appliances are:

- XTM 2 Series: XTM21, XTM22, XTM23, XTM21-W[7], XTM22-W, XTM23-W, XTM25, XTM25-W, XTM26, and XTM26-W;
- XTM 3 Series: XTM33, XTM33-W, and XTM330;
- XTM 5 Series: XTM505, XTM510, XTM520, and XTM530;
- XTM 8 Series: XTM610, XTM820, and XTM830-F;
- XTM 1050; and
- XTM 2050.

9 Documentation

The WatchGuard Technologies, Inc. documents provided to the consumer are as follows:

a. Fireware XTM Web UI 11.5.1 User Guide, 12/2/2011;

b. Fireware XTM WatchGuard System Manager 11.5.1 User Guide, 12/5/2011;

c. WatchGuard System Manager and Fireware XTM v11.5 Copyright and Licensing Guide, November 10, 2011;

d. WatchGuard® XTM 1050 Quick Start Guide;

e. WatchGuard® XTM 1050 Quick Start Guide;

[7] W" in the model number indicates wireless support; wireless support is not included in the evaluation.

f. Quick Start Guide WatchGuard® XTM 33;

g. Quick Start Guide WatchGuard® XTM 330;

h. WatchGuard® XTM 2 Series Quick Start Guide;

i. WatchGuard® XTM 5 Series Quick Start Guide; and

j. WatchGuard® XTM 8 Series Quick Start Guide.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of XTM Firewalls, including the following areas:

Development: The evaluators analyzed the XTM Firewalls functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the XTM Firewalls security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the XTM Firewalls 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 XTM Firewalls configuration management system and associated documentation was performed. The evaluators found that the XTM Firewalls configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of XTM Firewalls during distribution to the consumer.

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 XTM Firewalls 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 WatchGuard Technologies, Inc. for XTM Firewalls. 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 evaluators conducted an independent vulnerability analysis of XTM Firewalls. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to XTM Firewalls in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 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[8].

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, TOE design and security architecture description was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation,

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

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 is the following list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Audit of login failures: The objective of this test goal is to confirm the TOE generates audit records of login failures and that an administrator can review the records;

c. Backup and Restore: The objective of this test goal is to confirm the TOE performs backup and restore of data (policy data, audit data) to a USB drive; and

d. Cryptographic support: The objective of this test goal is to confirm SSL[9] must be used to access the TOE.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and a focused review of all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on port scanning, cross site scripting[10], and SQL injection[11].

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

11.4 Conduct of Testing

XTM Firewalls 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

[9] Secure Socket Layer, a protocol for encrypting information over the Internet.

[10] Cross-site scripting (XSS) is a type of vulnerability that enables attackers to inject client-side script into web pages viewed by other users.

[11] SQL injection is a code injection technique that exploits a security vulnerability when user input is incorrectly filtered .

activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that XTM Firewalls behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 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.

13 Evaluator Comments, Observations and Recommendations

The documentation for XTM Firewalls includes comprehensive Installation and Users Guides.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
USB	Universal Serial Bus
XTM	eXtensible Threat Management

15 References

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

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. U.S. Government Application-level Firewall In Basic Robustness Environments version 1.1, July 2007.

e. U.S. Government Traffic Filter Firewall In Basic Robustness Environments version 1.1, July 2007.

f. WatchGuard Technologies, Inc. XTM Firewalls and Fireware XTM Operating System v11.5.1 Security Target, v0.8, 13 April 2012.

g. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of WatchGuard Technologies, Inc. XTM Firewalls and Fireware XTM Operating System v11.5.1, Document No. 1658-000-D002, Version 1.3, 24 April 2012.