Swedish Certification Body for IT Security

Certification Report - WatchGuard

Issue: 1.0, 2017-maj-05

Authorisation: Jerry Johansson, Lead certifier , CSEC

Table of Contents

1 Executive Summary

The WatchGuard Firebox is an all-in-one network and content security boundary protection device.

The TOE consists of both software and hardware. The evaluation covers the Fireware v11.11.2.508770 operating system, running on a dedicated hardware appliance, and the WatchGuard Dimension 2.1 software for audit log viewing and sorting.

The ST does not claim conformance to any Protection Profiles (PPs).

There are four assumptions being made in the ST regarding the secure usage and environment of the TOE. The TOE relies on these to counter the eight threats and comply with the three organisational security policies (OSPs) in the ST. The assumptions, threats and OSPs are described in chapter 4 Assumptions and Clarification of Scope.

The evaluation has been performed by Combitech AB in Växjö and Sundbyberg, Sweden, partly with the assistance of Electronic Warfare Associates-Canada Ltd. In Ottawa, Canada. A site-visit has been performed in the developer's premises in Seattle, USA.

The evaluation was completed in 2017-04-11. The evaluation was conducted in accordance with the requirements of Common Criteria (CC) and the Common Methodology (CEM), version 3.1 release 4. The evaluation was performed at the evaluation assurance level EAL 4, augmented by ALC_FLR.2 Flaw Reporting Procedures.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB are also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria.

Electronic Warfare Associates-Canada Ltd. Operates as a Foreign Location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and by observing testing. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 4 augmented by ALC_FLR.2

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced byCombitech AB

> The certification results only apply to the versions of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.
>
> This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2015010
Name and version of the certified IT product	WatchGuard Firebox Security Appliances with Fireware v11.11 and WatchGuard Dimension 2.1
Security Target Identification	WatchGuard Fireware v11.11.2.508770 operating system running on one of the security appliances Fireware M200, Fireware M300, Fireware M400, Fireware M440, Fireware M500, Fireware M4600, Fireware M5600, Firebox T10, Firebox T10-W, Firebox T30, Firebox T30-W, Firebox T50, or Firebox T50-W. The WatchGuard Dimension 2.1 audit log viewing and sorting software.
EAL	EAL 4 + ALC_FLR.2
Sponsor	WatchGuard Technologies Inc.
Developer	WatchGuard Technologies Inc.
ITSEF	Combitech AB and EWA-Canada Ltd.
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
QMS version	1.20.3
Recognition Scope[1]	CCRA, SOGIS, EA/MLA
Certification date	2017-05-05

- [1]Until September 2017, the following text is used in CCRA certificates underneath the logo for products that has been awarded a certificate prior september 2014.
  ”CCRA recognition for components up to EAL 4 and ALC_FLR only”
- The following text is used in CCRA certificates underneath the logo for products that has not been awarded a certificate prior september 2014.
  ”CCRA recognition for components up to EAL 2 and ALC_FLR only”
- The following text is used in CCRA certificates underneath the logo for products claiming conformance against a cPP:
  [Ask C CSEC]
- The following text is always used on SOG-IS MRA certifiates underneath the logo:
  ”SOG-IS MRA recognition for components up to EAL 4 and ALC_FLR.1 only”

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

3.1 Security Audit

The Firebox devices generate audit entries for security related events which are stored as audit logs in the WatchGuard Dimension server. The audit logs are protected from unauthorized modification and deletion and may only be reviewed by authorized administrators.

3.2 Cryptographic Support

The TOE depends on FIPS validated cryptographic algorithms. The TOE protects the confidentiality and integrity of all information when it passes between the TOE and the remote management workstation, and also when it passes between the TOE and the local management workstation. The TOE achieves this by using validated cryptographic algorithms to perform encryption and the decryption of data according to the SSH and TLS protocols.

3.3 User Data Protection

Information flow control is achieved through the use of policy and policy enforcement.

3.4 Identification and Authentication

The TOE provides two pre-configured administrative accounts. The TOE requires that users associated with these accounts be identified and authenticated before permitted access to the TOE and TOE security functions. Users may authenticate using either local password authentication, or Active Directory.

3.5 Security Management

The TOE provides local management capabilities via serial connection and remote management capabilities via workstation CLI and/or Web-Based GUI. Management functions allow the administrators to configure users, roles, and security policy attributes.

3.6 Protection of the TSF

The operating system clock inside the TOE provides all of the timestamps for the audits.

3.7 Trusted Path/Channels

The communications links between the TOE and its remote administrators are protected using HTTPS (TLS v1.2) for the Web-based GUI and SSH (v2.0) for workstation CLI.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE.

A.MANAGE - There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.SECALG - Administrators will ensure that their browsers and SSH client applications use only approved cryptographic algorithms.

4.2 Environmental Assumptions

The Security Target [ST] makes two assumptions on the operational environment of the TOE.

A.LOCATE - The TOE hardware and software will be located within controlled access facilities and protected from unauthorized physical modification.

A.SINGEN - Information cannot flow among the internal and external networks unless it passes through the TOE.

4.3 Clarification of Scope

The Security Target contains eight threats, which have been considered during the evaluation.

T.ACCESS - An unauthorized person on an external network may attempt to by-pass the information flow control policy to access protected resources on the internal network.

T.AUDACC - Persons may not be accountable for the actions that they conduct because the audit records are not reviewed, or records have been compromised, thus allowing an attacker to escape detection.

T.COMDIS - An unauthorized user may attempt to disclose the data collected by the TOE by bypassing a security mechanism.

T.MEDIAT - An unauthorized person may send impermissible information through the TOE that result in the exploitation of resources on the internal network.

T.NOAUTH - An unauthorized person may attempt to bypass the security of the TOE so as to assess and use security functions and/or non- security functions provided by the TOE.

T.NOHALT - An unauthorized user may attempt to compromise the continuity of the TOE functionality by halting execution of the TOE.

T.PRIVIL - An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

T.PROCOM - An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information that is sent between a remotely located authorized administrator and the TOE.

The Security Target contains three Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.ACCACT - Users of the TOE shall be accountable for their actions.

P.DETECT - All events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity must be collected.

P.MANAGE - The TOE shall be manageable only by authorized administrators.

5 Architectural Information

The TOE consists of the WatchGuard Fireware v11.11.2.508770 operating system, running on one of the security appliances:

Fireware M200, Fireware M300, Fireware M400,
Fireware M440, Fireware M500, Fireware M4600,
Fireware M5600, Firebox T10, Firebox T10-W,
Firebox T30, Firebox T30-W, Firebox T50, or
Firebox T50-W.

and the WatchGuard Dimension 2.1 audit log viewing and sorting software.

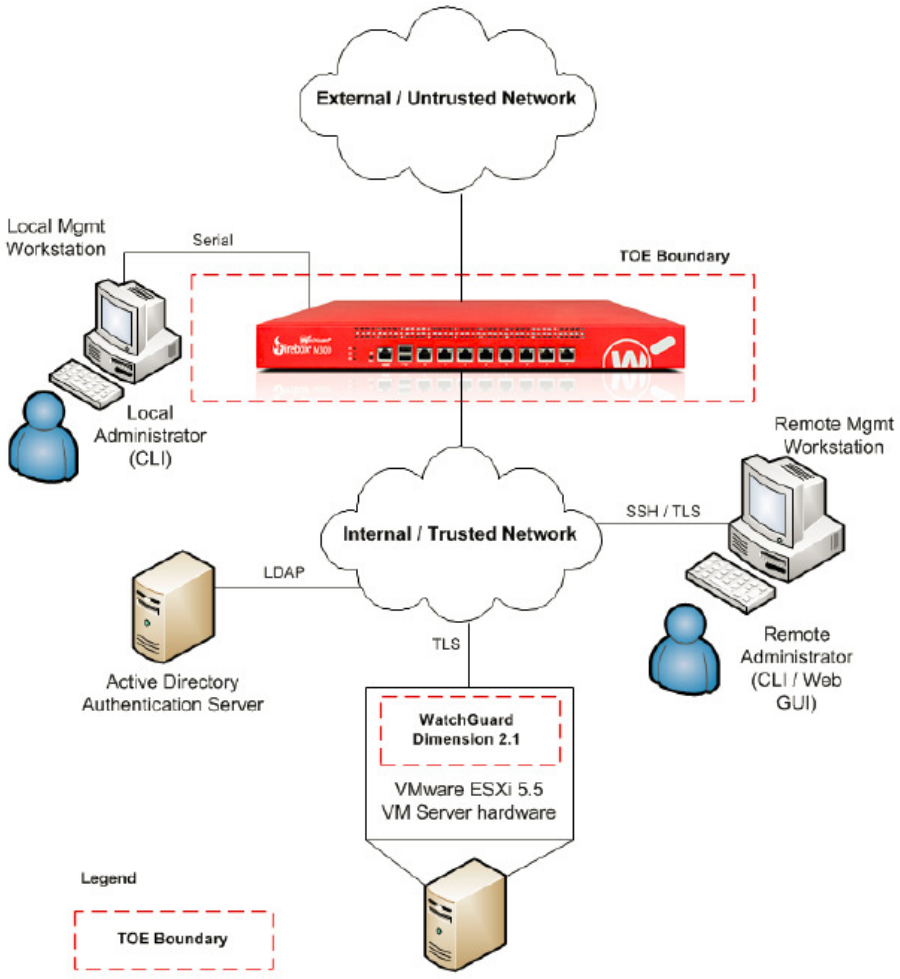

Figure 1, The TOE parts in a typical operational environment.

6 Documentation

The following documents are included in the scope of the TOE:

WatchGuard Firebox Security Appliances with Fireware v11.11 Guidance Supplement

Fireware Command Line Interface Reference

WatchGuard Firebox M200/M300 Hardware Guide

WatchGuard Firebox M400/M500 Hardware Guide

WatchGuard Firebox M440 Hardware Guide

WatchGuard Firebox M4600 Hardware Guide

WatchGuard Firebox M5600 Hardware Guide

WatchGuard Firebox T10 Hardware Guide

WatchGuard Firebox T30/T50 Hardware Guide

WatchGuard Firebox M200/M300 Quick Start Guide

WatchGuard Firebox M400/M500 Quick Start Guide

WatchGuard Firebox M440 Quick Start Guide

WatchGuard Firebox M4600 Quick Start Guide

WatchGuard Firebox M5600 Quick Start Guide

WatchGuard Firebox T10/T10-W Quick Start Guide

WatchGuard Firebox T30, T30-W/T50, T50-W Quick Start Guide

7 IT Product Testing

7.1 Developer Testing

The developer tested all variants of the TOE. All SFRs were covered by the external testing. Some testing of internal interfaces, i.e. direct calls to cryptographic primitives, was covered in the form of evidence from FIPS CAVP testing.

7.2 Evaluator Testing

The evaluators repeated a subset of the developer tests, on the T30, T30-W, M440 and M5600 hardware appliances. A number of complementary test were added, testing the cryptographic SFRs thoroughly against independent implementations of the primitives, modes schemes and protocols.

7.3 Penetration Testing

The evaluators put particular emphasis in identifying third party modules and to eliminate potential vulnerabilities for those. The penetration testing focused on port scanning (NMAP), and vulnerability scanning (Nessus and Armitage). The penetration tests were performed on the T30, T30-W, M440 and M5600 hardware appliances.

8 Evaluated Configuration

The installation and setup of the evaluated configuration is described in [INST].

Note that the following features are not included in the evaluated configuration:

External Network Interface – The external network interface allows for remote administration of the TOE. Authorized administrators can connect to the TOE through the external network and configure the TOE, monitor its operation, and examine the audit logs via remote workstation by logging into a Web-based GUI. To protect the confidentiality and integrity of information the external network connection must be configured to allow HTTPS and TLS (v1.2) at the network port and the remote web browser respectively. The External Network Interface is not to be used in the evaluated configuration.

Telnet – Use of Telnet protocol is not permitted in the evaluated configuration of the TOE.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of enhanced-basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class/Family	*Short name*	*Verdict*
Development	ADV	PASS
Security Architecture	ADV_ARC.1	PASS
Functional Specification	ADV_FSP.4	PASS
Implementation Representation	ADV_IMP.1	PASS
TOE Design	ADV_TDS.3	PASS
Guidance Documents	AGD	PASS
Operational User Guidance	AGD_OPE.1	PASS
Preparative Procedures	AGD_PRE.1	PASS
Life-cycle Support	ALC	PASS
CM Capabilities	ALC_CMC.4	PASS
CM Scope	ALC_CMS.4	PASS
Delivery	ALC_DEL.1	PASS
Development Security	ALC_DVS.1	PASS
Life-cycle Definition	ALC_LCD.1	PASS
Tools and Techniques	ALC_TAT.1	PASS
Flaw Remediation	ALC_FLR.2	PASS
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance Claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security Objectives	ASE_OBJ.2	PASS
Extended Components Definition	ASE_ECD.1	PASS
Security Requirements	ASE_REQ.2	PASS
TOE Summary Specification	ASE_TSS.1	PASS
Tests	ATE	PASS
Coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional Tests	ATE_FUN.1	PASS
Independent Testing	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability Analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
TSF	TOE Security Functionality
TCBC	TDEA Cipher Block Chaining

12 Bibliography

ST	WatchGuard Firebox Security Appliances with Fireware v11.11 Security Target, WatchGuard, 2016-10-17, document version 1.3
INST	WatchGuard Firebox Security Appliances with Fireware v11.11 Guidance Supplement, EWA-Canada and WatchGuard, 2016-08-31, v1.0
CLI	Fireware Command Line Interface Reference, WatchGuard, 2016, version 11.11.4
HG M200/300	WatchGuard Firebox M200/M300 Hardware Guide, WatchGuard, 2015-06-01
HG M400/500	WatchGuard Firebox M400/M500 Hardware Guide, WatchGuard, 2015-03-10
HG 440	WatchGuard Firebox M440 Hardware Guide, WatchGuard, 2015-07-14
HG M4600	WatchGuard Firebox M4600 Hardware Guide, WatchGuard, 2016-02-11
HG M5600	WatchGuard Firebox M5600 Hardware Guide, WatchGuard, 2016-02-11
HG T10	WatchGuard Firebox T10 Hardware Guide, WatchGuard, 2015-02-11
HG T30/50	WatchGuard Firebox T30/T50 Hardware Guide, WatchGuard, 2016-02-11
QG M200/300	WatchGuard Firebox M200/M300 Quick Start Guide, WatchGuard, 2016-01-13, Rev A
QG M400/500	WatchGuard Firebox M400/M500 Quick Start Guide, WatchGuard, 2015-10-02, Rev B
QG M440	WatchGuard Firebox M440 Quick Start Guide, WatchGuard, 2015-07-22, Rev D
QG M4600	WatchGuard Firebox M4600 Quick Start Guide, WatchGuard, 2016-01-28, Rev A
QG M5600	WatchGuard Firebox M5600 Quick Start Guide, WatchGuard, 2016-01-28, Rev A
QG T10	WatchGuard Firebox T10/T10-W Quick Start Guide, WatchGuard, 2014-08-21, Rev D
QG T30/50	WatchGuard Firebox T30, T30-W/T50, T50-W Quick Start Guide, WatchGuard, 2016-02-12, Rev B
CCpart1	Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 4, CCMB-2012-09-001
CCpart2	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-002
CCpart3	Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 4, CCMB-2012-09-003

CC	CCpart1 + CCpart2 + CCpart3
CEM	Common Methodology for Information Technology Security Evaluation, version 3.1 revision 4, CCMB-2012-09-004

Appendix A Scheme Versions

A.1 Scheme/Quality Management System

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme has been used:

Version	Introduced	Impact of changes
1.20.3	2017-04-24	*None*
1.20.2	2017-02-27	*None*
1.20.1	2017-01-12	*None*
1.20	2016-10-20	*None*
1.19.3	Application	Initial version

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system. The changes between consecutive versions are outlined in "Ändringslista QMS 1.20.3". The certifier concluded that, from QMS 1.19.3 to the current QMS 1.20.3, there are no changes with impact on the result of the certification.

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Demonstration of test coverage
- Scheme Note 18 - Highlighted Requirements on the Security Target