Reference: 2018-26-INF-3091-v1
Target: Público
Date: 01.06.2020

Created by: CERT10
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2018-26**
TOE	**WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software**
Applicant	**911712427 - WatchGuard Technologies Inc.**
References	
	[EXT-4197] Certification request
	[EXT-5778] Evaluation Technical Report

Certification report of the product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software, as requested in [EXT-4197] dated 27/07/2017, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-5778] received on 14/02/2020.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software.

The TOE is designed to filter network traffic based on a set of rules that are created by a system administrator. It separates the organization's internal networks from external network connections to decrease the risk of an external attack. It protects the internal, private networks from unauthorized users on the Internet. The TOE examines traffic that enters and leaves the protected networks. Access policies identify and filter different types of information and can control which policies or ports the protected computers can use on the Internet (outbound access).

The TOE has extensive logging capabilities which include the logging of administrative actions and security related network events. The WatchGuard Dimension 2.1.2 software provides for viewing and sorting of audit logs.

The TOE is a software only TOE. It is supported by the WatchGuard Firebox appliance hardware, which is in the operational environment.

Developer/manufacturer: WatchGuard Technologies Inc.

Sponsor: WatchGuard Technologies Inc..

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r5 – EAL4 + ALC_FLR.2.

Evaluation end date: 05/03/2020.

Expiration Date[1]: 30/05/2025

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4, as defined by the Common Criteria v3.1 r5 and the CEM v3.1 r5.

Considering the obtained evidences during the instruction of the certification request of the product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software, a positive resolution is proposed.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

TOE SUMMARY

The TOE is designed to filter network traffic based on a set of rules that are created by a system administrator. It separates the organization's internal networks from external network connections to decrease the risk of an external attack. It protects the internal, private networks from unauthorized users on the Internet. The TOE examines traffic that enters and leaves the protected networks. Access policies identify and filter different types of information and can control which policies or ports the protected computers can use on the Internet (outbound access).

The TOE has extensive logging capabilities which include the logging of administrative actions and security related network events. The WatchGuard Dimension 2.1.2 software provides for viewing and sorting of audit logs.

The TOE is a software only TOE. It is supported by the WatchGuard Firebox appliance hardware, which is in the operational environment.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 r5.

Assurance Class	**Assurance components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification

ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 r5 and the CEM v3.1 r5:

Functional Class	**Class name**
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FAU_STG.4	Prevention of audit data loss
FAU_GEN.1	Audit data generation
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key Destruction
FCS_COP.1	Cryptographic operation
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FIA_AFL.1	Authentication failure handling
FIA_UAU.1	Timing of authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1(1)	Security roles (Fireware OS)
FMT_SMR.1(2)	Security Roles (Dimension)
FPT_STM.1	Reliable time stamps
FTP_TRP.1	Trusted path

IDENTIFICATION

Product: WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software

Security Target: WatchGuard Fireware OS v12.3.1 (Running on Firebox Security Appliances) Security Target, version 1.6, 14 November 2019.

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 r5 – EAL4 + ALC_FLR.2.

SECURITY POLICIES

The use of the product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.2 (Organisational Security Policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.3 (Assumptions), are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.1 (Threats) do not suppose a risk for the product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are detailed in [ST], chapter 4.2 (Security Objectives for the Operational Environment).

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The table below summarizes the logical scope of the TOE.

Functional Classes	**Description**
Security Audit	The TOE generates 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.
Cryptographic Support	The TOE depends on FIPS validated cryptographic algorithms, as detailed in Table 13. The TOE protects the confidentiality and integrity of all information when it passes between the TOE and the remote 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.
User Data Protection	Information flow control is achieved through the use of policy and policy enforcement.
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.
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.

Protection of the TSF	Reliable time stamps are provided in support of the audit functions.
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.

PHYSICAL ARCHITECTURE

The Figure 1 shows the physical architecture of the TOE in their evaluated configuration.

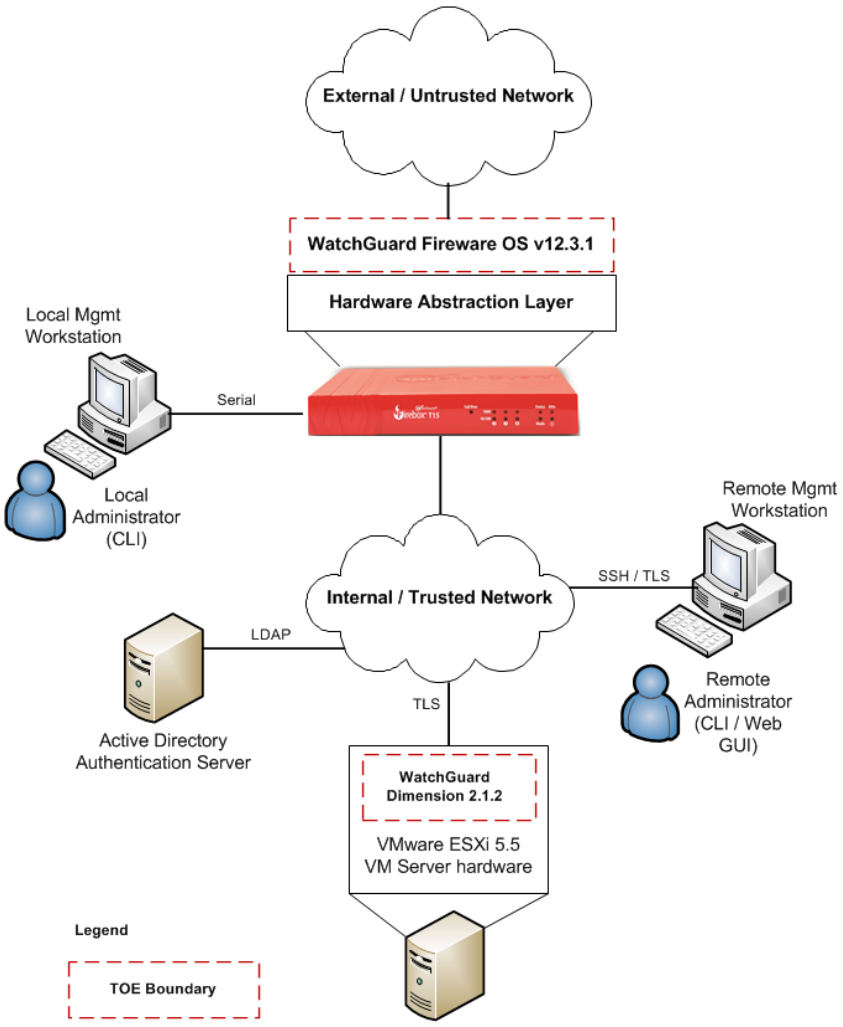

Figure 1: Physical architecture of the TOE

The TOE consists of these two software components:

- **Fireware OS version 12.3.1**, which is preloaded on each appliance prior to shipping. It is also available on:
    - Download URL: https://watchguardsupport.secure.force.com/software/SoftwareDownloads?familyId=a2R2A000002amFiUAI (Fireware v12.3.1 Update 1)
    - Filename: Firebox_OS_T35_12_3_1_U1.exe
    - Hash (SHA-256): c129587985e5d7daddda748e73f6028e4fcaca81460f4bbf3db9a0fc6ef08980
- **WatchGuard Dimension 2.1.2 software**, which is operated on an independent virtual machine in the operational environment. It is available on:
    - Download URL: http://cdn.watchguard.com/SoftwareCenter/Files/WSM/2_1_2/watchguard-dimension_2_1_2.ova
    - Filename: watchguard-dimension_2_1_2.ova
    - Hash (SHA-256): 8f294d29466b3d9d67fc2c64ea09fb10f8d9e122f23032127fbbd288fc79f92f

In addition, all the documents listed in section *DOCUMENTS* are part of the physical scope of the TOE.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- **Fireware Help** is provided in HTML format and can be downloaded as a zip file from the following location:
    - https://www.watchguard.com/help/FIPS_Help_Center_12_3_1/Help-Center_(en-US)_v12-3-1.zip
- **Fireware Command Line Interface Reference** is provided in Portable Document Format (PDF) and can be downloaded from the following location:
    - https://www.watchguard.com/help/docs/fireware/12/en-US/CLI/CLI_Reference_v12_3.pdf
- Also, a Common Criteria Guidance Supplement is also available to customers, in PDF format, upon request:

- WatchGuard Fireware OS v12.3.1 (Running on Firebox Security Appliances), **Guidance Supplement, Version 1.5**

PRODUCT TESTING

The developer has executed test for all the functionalities and security mechanisms of TOE, covering all TSFIs and SFRs. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each test case checking that the security functionality that covers is been identified and that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator has repeated all the developer functional tests in the developer premises.

Regarding the independent testing plan, the evaluator's approach has been to prioritize the coverage of SFRs that have a great impact in the overall security of the TSF resulting in a coverage of around 70%. Nevertheless, all the TSFIs have been covered in the test subset devised by the evaluator.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals (see *DOCUMENTS* section of this certification report.

Among all the hardware models supported by the TOE, the evaluator selected:

- **Firebox Security Appliance: Firebox T35/T35-W**.

The other HW/SW non-TOE components selected for the evaluation were:

- Local Management Workstation: Terminal Application operating in VT100 emulation mode, connected to the TOE through the serial port.

- Remote management Workstation: a computer supporting SSH v2.0 (for CLI) and TLS v1.2 (for GUI).
- Active Directory Authentication Server: Windows 2012 R2 virtualized in Proxmox Virtualization Server.
- WatchGuard Dimension environmental support: VMWare Virtualization Server.

EVALUATION RESULTS

The product WatchGuard Fireware OS v12.3.1.B585922 (Running on Firebox Security Appliances) with WatchGuard Dimension 2.1.2.B588050 Software has been evaluated against the Security Target: WatchGuard Fireware OS v12.3.1 (Running on Firebox Security Appliances) Security Target, version 1.6, 14 November 2019.

All the assurance components required by the evaluation level EAL4+ (ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4+ (ALC_FLR.2), as defined by the Common Criteria v3.1 r5 and the CEM v3.1 r5.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

There is no additional recommendation from the evaluation team in order to use the TOE since guidance documentation is enough to make a secure usage of the TOE.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Applus Laboratories, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] WatchGuard Fireware OS v12.3.1 (Running on Firebox Security Appliances) Security Target, version 1.6, 14 November 2019.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- WatchGuard Fireware OS v12.3.1 (Running on Firebox Security Appliances) Security Target, version 1.6, 14 November 2019.

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for assurance components up to EAL4.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand,

Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components up to EAL2 and ALC_FLR.