TÜVRheinland®
Precisely Right.

Certification Report

Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server

Sponsor and developer: ***Check Point Software Technologies Ltd.***
Shlomo Kaplan St 5
Tel Aviv-Yafo
Israel

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0046947-CR**

Report version: **1**

Project number: **0046947**

Author(s): **Kjartan Jæger Kvassnes**

Date: **23 December 2019**

Number of pages: **11**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server. The developer of the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server is Check Point Software Technologies Ltd. located in Tel Aviv-Yafo and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a managed packet filtering firewall application, with IPS pattern matching (software) blade. The TOE provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 20 December with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target [ST], which identifies assumptions made during the evaluation, the intended environment for the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server, 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 Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server 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 *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL4 augmented with ALC_FLR.1 (Basic Flaw Remediation) assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server from Check Point Software Technologies Ltd. located in Tel Aviv-Yafo.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Check_Point_R80.30_T200_Security_Management.iso with Check_Point_R80.30_T200_Hotfix_T6_sk162814_FULL.tgz	R80.30
Software	Check_Point_R80.30_T200_Security_Gateway.iso with Check_Point_R80.30_T200_Hotfix_133_T6_sk162814_FULL.tgz	R80.30
Software	Check_Point_R80.30_Gaia_3.10_T273.iso with Check_Point_R80.30_T300_GAIA_3.10_Hotfix_020_T6_sk162814_FULL.tgz	R80.30

To ensure secure usage a set of guidance documents is provided together with the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server. Details can be found in section “Documentation” of this report.

2.2 Security Policy

The TOE is a managed packet filtering firewall application, with IPS pattern matching (software) blade. The TOE provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

The Management Server and management workstation are co-located on a logically protected LAN behind the firewall.

The purpose of the firewall blade is to protect the assets operating on a customer’s network from malicious attempts to control or gain access to those assets. The IPS pattern matching blade provides protection against signatures defining malicious and unwanted network traffic, focusing on application and server vulnerabilities, as well as in-the-wild attacks by exploit kits and malicious attackers. The firewall filtering rules, and IPS rules are defined, managed and deployed by the Security Management Server.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.3 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

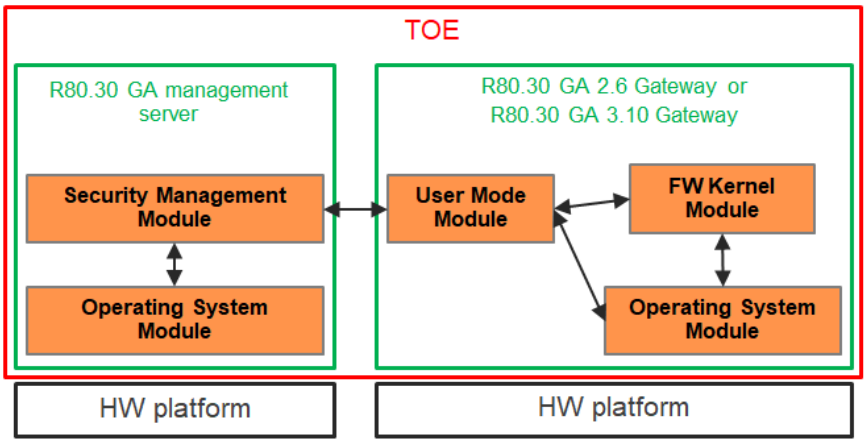
The TOE is a managed packet filtering firewall application, with IPS pattern matching (software) blade. The TOE provides controlled connectivity between two or more network environments. It mediates information flows between clients and servers located on internal and external networks governed by the firewalls.

The TOE is a software TOE and its components execute on hardware platforms identified in the [ST]. These platforms are provided by the Operational Environment.

The TOE includes the following components:

- Security Management server
  - The Management Server handles policy, log, alert and system status data flows. In handling the policy data flow, it receives policy data entered via the Check Point Management API by the TOE administrator, and processes (compiles), stores and distributes it to the Security Gateway. In handling the log and alert data flow, it receives data from the Gateway, and processes, stores and conveys it to the TOE administrator. In handling the system status data flow, it passes queries from the Management API to the Gateway and query results from the Gateway to the Management API.
- Security Gateway
  - The Gateway is the policy enforcement point for traffic flowing through the TOE. Traffic filtering is performed by kernel-level code to ensure maximum performance. User-level components perform tasks which the kernel cannot: write-to-file, log handling, inter-host communication and management.

The logical architecture of the TOE can be depicted as follows:



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
R80.30 CC Installation Configuration Admin Guide	(101219)

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has tested all TSFIs. The evaluator repeated all the automated test cases detailed in the developer's test plan and sampled the manual test case.

2.6.2 Independent Penetration Testing

The following focused vulnerability analysis was used by the evaluator to identify potential vulnerabilities:

- Focused search: An analysis of the evidence with the aim of identifying any potential vulnerabilities evident through the contained information. The evaluator used their knowledge of the TOE design and operation gained from the TOE deliverables to conduct a flaw hypothesis to identify potential flaws in the development of the TOE and potential errors in the specified method of operation of the TOE.
- Generic vulnerabilities: The evaluator considers generic vulnerabilities defined in the CEM (bypassing, tampering, direct, monitoring and misuse vulnerabilities). During this examination several potential vulnerabilities were identified.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- Network scanning tools: The evaluator ran vulnerability scanning tools to identify potential vulnerabilities. The tools assist the evaluator in assuring that the public domain search is complete.
- Static code analysis: The developer provide the results of static code analysis. The evaluator reviewed the findings.

The identified potential vulnerabilities were analysed, and some of the potential vulnerabilities were covered by guidance or by implementation checks. For remaining potential vulnerabilities, penetration tests were devised.

The evaluator focused on the following:

- Disabled features
- Bypassing the firewall rule base
- Bypassing user authentication
- TOE initialisation
- Fail-safe mode of the Firewall Kernel
- Use of memset
- Firewall policy installation
- Concurrent administration sessions

Local audit log storage

2.6.3 Test Configuration

The developer has two environments (automated and manual) that are used for testing. The environments contained the following:

- Automated:
  - Smart-1 405 Security Management appliance running R80.30 GA Security Management Server with HF: Check_Point_R80.30_T200_Hotfix_T6_sk162814_FULL.tgz
  - 6500 Security Gateway appliance running R80.30 GA 2.6 Gateway with HF: Check_Point_R80.30_T200_Hotfix_133_T6_sk162814_FULL.tgz
- Manual:
  - Smart-1 405 Security Management appliance running R80.30 GA Security Management Server with HF: Check_Point_R80.30_T200_Hotfix_T6_sk162814_FULL.tgz

26000 Security Gateway appliance running R80.30 GA 3.10 Gateway with HF: Check_Point_R80.30_T300_GAIA_3.10_Hotfix_020_T6_sk162814_FULL.tgz.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.1**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation.

3 Security Target

The Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server Security Target, 10 December 2019 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] Check Point Software Technologies Ltd. R80.30 Firmware for Security Gateway Appliances with Firewall, IPS Blade Pattern Matcher, and Security Management Server Security Target, 10 December 2019.

(This is the end of this report).