# Certification Report

## Check Point R81.10 for Gateway and Maestro Configurations

| | |
|---|---|
| Sponsor and developer: | ***Check Point Software Technologies Ltd.***<br>**Shlomo Kaplan St 5**<br>**67897 Tel Aviv-Yafo**<br>**Israel** |
| Evaluation facility: | ***SGS Brightsight B.V.***<br>**Brassersplein 2**<br>**2612 CT Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-0373888-CR** |
| Report version: | **1** |
| Project number: | **0373888** |
| Author(s): | **Kjartan Jæger Kvassnes** |
| Date: | **06 December 2022** |
| Number of pages: | **12** |
| Number of appendices: | **0** |





Head Office:
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 Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

TÜVRheinland®
Precisely Right.

# CONTENTS

TÜVRheinland®
Precisely Right.

## 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 licence 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, 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

TÜVRheinland®
Precisely Right.

# Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

## International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

## European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Check Point R81.10 for Gateway and Maestro Configurations. The developer of the Check Point R81.10 for Gateway and Maestro Configurations is Check Point Software Technologies Ltd. located in Tel Aviv, Israel 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 the Security Gateway Appliances R81.10 firmware providing firewall capabilities for filtering traffic based on packet rules and IPS pattern matching. It is a distributed system with support for a security management server deployed on a dedicated management LAN behind the firewall.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 01 December 2022 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 R81.10 for Gateway and Maestro Configurations, 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 R81.10 for Gateway and Maestro Configurations 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 provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.1 (Basic flaw remediation).

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]* (Parts I, II and III).

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. Note that the certification results apply only 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 available 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 R81.10 for Gateway and Maestro Configurations from Check Point Software Technologies Ltd. located in Tel Aviv, Israel.

The TOE is comprised of the following main components:

| Delivery item type | Identifier | Version |
|---|---|---|
| Software | Security Gateway or Management Server | R81.10 |
| | Scalable Platform (Maestro) Gateway and Maestro Hyperscale Orchestrator | R81.10 |
| | R81.10 EAL4 certification Hotfix | R81.10 |

The TOE requires hardware platforms for it to operate, but these are not part of the TOE; they exist within the TOE environment. These hardware platforms are Check Point Security Gateway Appliances/Security Gateway Modules and Security Management Appliances, which execute firmware installed from the applicable R81.10 firmware image, and the Orchestrator appliances if the TOE is deployed as a Scalable Platform.

The hardware platforms are as follows:

- Maestro appliances running R81.10 firmware (Scalable Platform image):
  - Maestro Hyperscale Gateway

    6200, 6600, 6700, 7000, 16600, 28600
- Security Gateway appliances running R81.10 firmware (Security Gateway appliance image):
  - High End Enterprise Data Center:

    16000, 16200, 26000, 28000, 28600, 16600
  - Enterprise:

    6200, 6400, 6500, 6600, 6700, 6900, 7000
  - Small Business and Branch Offices:

    3600, 3800
- Virtual appliances running R81.10 firmware (VM image including the Security Gateway appliance firmware image):
  - CloudGuard for ESXi running on a HPE D360 G10
- Smart-1 Security Management Server appliances running the GAiA R81.10 firmware(Security Management Server image):
  - High End Enterprise:

    625, 600-M, 600-S, 6000-L, 6000-XL
- Orchestrator appliances
  - Maestro Hyperscale Orchestrator 140
  - Maestro Hyperscale Orchestrator 170
  - Maestro Hyperscale Orchestrator 175

To ensure secure usage a set of guidance documents is provided, together with the Check Point R81.10 for Gateway and Maestro Configurations. For details, see section 2.5 “Documentation” of this report.

## 2.2 Security Policy

The TOE is a combination of the firmware for Security Gateway Module(s), a Security Management Server and (when deployed in Scalable Platform configuration) the firmware for the Maestro Orchestrator appliance(s):

- The Security Gateway Module (SGM) 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 SGM can either be deployed using instances of a single Security Gateway appliance, which incorporates the SGM or a combination of Security Gateway Modules (SGM) operating in a cluster as part of a Scalable Platform (SP).
- The Security Management Server is used to manage and deploy the security policies and rules to SGM.
- When operating as part of a Scalable Platform (SP), the Orchestrator appliance provides load balancing services for the SGMs.

The Security Management Server is located on a logically protected LAN behind the firewall in single deployment mode, and behind the load-balancing Orchestrator in Scalable deployment mode. All management traffic is communicated between TOE components over secured channels provided by the TOE.

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. When in Scalable Deployment, the Orchestrator appliance(s) provide load-balancing across the gateway resources.

## 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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 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 combination of the firmware for Security Gateway Module(s), a Security Management Server and (when deployed in Scalable Platform configuration) the firmware for the Maestro Orchestrator appliance(s):

- The Security Gateway Module (SGM) 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 SGM can either be deployed using instances of a single Security Gateway appliance, which incorporates the SGM or a combination of Security Gateway Modules (SGM) operating in a cluster as part of a Scalable Platform (SP).
- The Security Management Server is used to manage and deploy the security policies and rules to SGM.
- When operating as part of a Scalable Platform (SP), the Orchestrator appliance provides load balancing services for the SGMs.

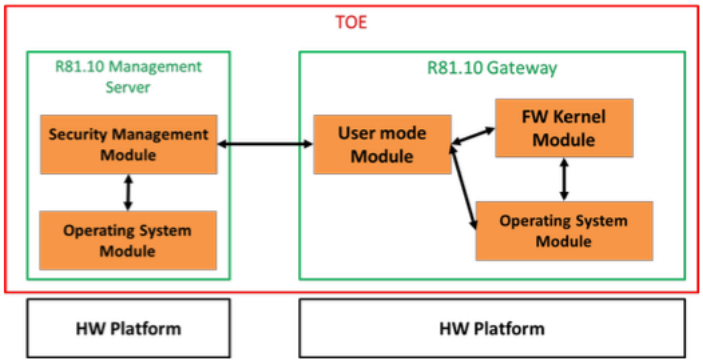


**Figure 1: Logical architecture of the TOE in single appliance deployment**

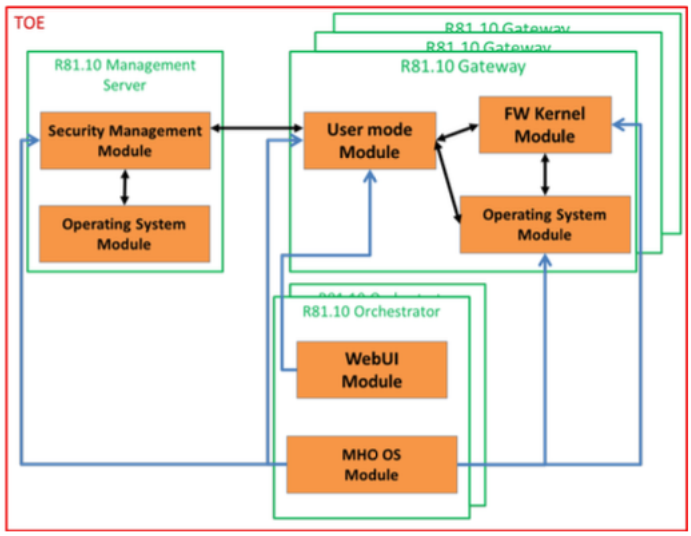


**Figure 2: Logical architecture of the TOE in Scalable Platform deployment (Management server, Gateway, and Orchestrators have their own hardware platform, not shown in the figure)**

## *2.5 Documentation*

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

| Identifier | Version |
|---|---|
| R81.10 CC Firmware for Gateway and Maestro Configurations, Installation and Configuration, Administration Guide, dated 20 October 2022 | Rev 002 |

## *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 performed tests on all the SFRs / TSFIs by using a combination of automatic and manual test approaches. The manual test REST API commands are initiated through the Postman tool. The automatic tests framework can be used to create scripts to automatically test different scenarios and reports can be automatically generated. As a result the automated test cases covered all the secure gateway TSFIs, while the manual tests are used to cover the WebUI for the Orchestrator and SIC between the TOE components.

The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

### 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.

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 total test effort expended by the evaluators was 80 hours. During that test campaign, 100% of the total time was spent on logical tests.

### 2.6.3 Test configuration

Two environments (automated and manual) were used for testing. Both environments contain the following hardware appliances:

- Check Point Smart-1 405 Security Management server
- Security Gateway 6500 Server
- Virtual Machine (also acted as Gateway)
- 2* Security Gateway 16600HS Server (for SP deployment)
- Maestro Hyperscale Security Orchestrator 140 (for the SP deployment)

All devices are running R81.10 firmware with hotfix as specified in the *[ST]*. The developer performed their tests on the Security Gateway 6500 server as well as the Virtual machine.

### 2.6.4 Test 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 Reused Evaluation Results*

There is no reuse of evaluation results in this certification.

## *2.8 Evaluated Configuration*

The TOE is defined uniquely by its name and version number Check Point R81.10 for Gateway and Maestro Configurations.

## 2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents, and Site Technical Audit Report(s) for the site(s) *[STAR]* [2].

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

Based on the above evaluation results the evaluation lab concluded the Check Point R81.10 for Gateway and Maestro Configurations, 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]*.

## 2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the customer 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. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>, which are out of scope as there are no security claims relating to these.

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

# 3 Security Target

The Check Point R81.10 for Gateway and Maestro Configurations  Common Criteria EAL4+ALC_FLR.1  Security Target , Revision 021 Dated 20 October 2022 *[ST]* is included here by reference.

# 4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

| | |
|---|---|
| IPS | Intrusion Prevention Systems |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| JIL | Joint Interpretation Library |
| LAN | Local Area Network |
| NSCIB | Netherlands Scheme for Certification in the area of IT Security |
| PP | Protection Profile |
| SGM | Security Gateway Module |
| SP | Scalable Platform |
| 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 R81.10 for Gateway and Maestro Configurations” – EAL4+, 21-RPT-254, Version 2.0, 22 November 2022 |
| [NSCIB] | Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019 |
| [ST] | Check Point R81.10 for Gateway and Maestro Configurations Common Criteria EAL4+ALC_FLR.1 Security Target , Revision 021 Dated 20 October 2022 |
| [STAR] | Site Technical Audit Report Tel Avis Check Point R81.10 for Gateway and Maestro Configurations, 22-RPT-1196, Version 2.0, Dated 22 November 2022 |


(This is the end of this report.)