National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00

Report Number: CCEVS-VR-11235-2022
Dated: March 21, 2022
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell
Jenn Dotson
Sheldon Durrant
Lisa Mitchell
Ben Schmidt
The MITRE Corporation

Farid Ahmed
Johns Hopkins University Applied Physics Laboratory

Common Criteria Testing Laboratory

Kevin Cummins
Ed Morris
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary ... 1
2 Identification ... 1
3 Architectural Information ... 3
3.1 TOE Evaluated Platforms ... 3
3.2 TOE Architecture ... 3
3.3 Physical Boundaries ... 4
4 Security Policy ... 4
4.1 Security audit ... 5
4.2 Communication ... 5
4.3 Cryptographic support ... 5
4.4 User data protection ... 5
4.5 Stateful Traffic Filtering Firewall ... 5
4.6 Identification and authentication ... 6
4.7 Security management ... 6
4.8 Packet filtering ... 6
4.9 Protection of the TSF ... 6
4.10 TOE access ... 7
4.11 Trusted path/channels ... 7
5 Assumptions ... 7
6 Clarification of Scope ... 7
7 Documentation ... 8
8 IT Product Testing ... 8
8.1 Developer Testing ... 8
8.2 Evaluation Team Independent Testing ... 8
9 Results of the Evaluation ... 9
9.1 Evaluation of the Security Target (ASE) ... 9
9.2 Evaluation of the Development (ADV) ... 9
9.3 Evaluation of the Guidance Documents (AGD) ... 9
9.4 Evaluation of the Life Cycle Support Activities (ALC) ... 10
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) ... 10
9.6 Vulnerability Assessment Activity (VAN) ... 10
9.7 Summary of Evaluation Results ... 11
10 Validator Comments/Recommendations ... 11
11 Annexes ... 11
12 Security Target ... 11
13 Glossary ... 11
14 Bibliography ... 12

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of Check Point Security Gateway and Maestro Hyperscale Appliances R81.00 provided by Check Point Software Technologies Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in March 2022. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the *collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020 with the *PP-Module for Stateful Traffic Filter Firewalls*, version v1.4 + Errata 20200625, 25 June 2020 and the *PP-Module for Virtual Private Network (VPN) Gateways*, version 1.1, 18 June 2020.

The TOE is the Check Point Security Gateway and Maestro Hyperscale Appliances R81.00. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00 Security Target*, version 0.5, March 16, 2022, and analysis performed by the Validation team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology

(CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Check Point Security Gateway and Maestro Hyperscale Appliances R81.00 (Specific models identified in Section 3.1)
Protection Profile	*collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020 with the *PP-Module for Stateful Traffic Filter Firewalls*, version v1.4 + Errata 20200625, 25 June 2020 and the *PP-Module for Virtual Private Network (VPN) Gateways*, version 1.1, 18 June 2020
ST	*Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00 Security Target*, version 0.5, March 16, 2022
Evaluation Technical Report	*Evaluation Technical Report for Check Point Security Gateway and Maestro Hyperscale Appliances R81.00*, version 0.3, March 17, 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Check Point Software Technologies Ltd.
Developer	Check Point Software Technologies Ltd.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Farid Ahmed, Paul Bicknell, Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Ben Schmidt

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is Check Point Software Security Gateway and Maestro Hyperscale Appliances running software version R81.00. Throughout the remainder of this document the Security Gateway appliances and the Maestro Hyperscale appliances are collectively referred to as “Gateways” or “Gateway appliances”. The product family is a set of VPN Gateway and packet filtering firewall appliances, a management appliance, and management software. The product 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.

3.1 TOE Evaluated Platforms

Below is a list of hardware platforms included in the evaluation. All products are running Checkpoint version R81.00 software. All platforms are x86 based hardware. These platforms can be installed as a Security Gateway or a Standalone (i.e., a combination of a Security Management Server and a Security Gateway on a single hardware platform) and all are running the R81.00 software.

- Check Point 3600, 3800
- Check Point 6200, 6400, 6600, 6700, 6900
- Check Point 7000
- Check Point 154**, 156**
- Check Point 16000, 16200, 16600
- Checkpoint 26000, 28000, 28600
- ESXi 7.0 (HPE D360 G10)

The following Check Point “Smart-1” Security Management Servers are included in the evaluated configuration, running the same R81.00 software. The below platform and virtualized platform run the same software but provide Security Management Server functionality and do not operate as a Security Gateway.

- Smart-1 525
- ESXi 7.0 (HPE D360 G10)

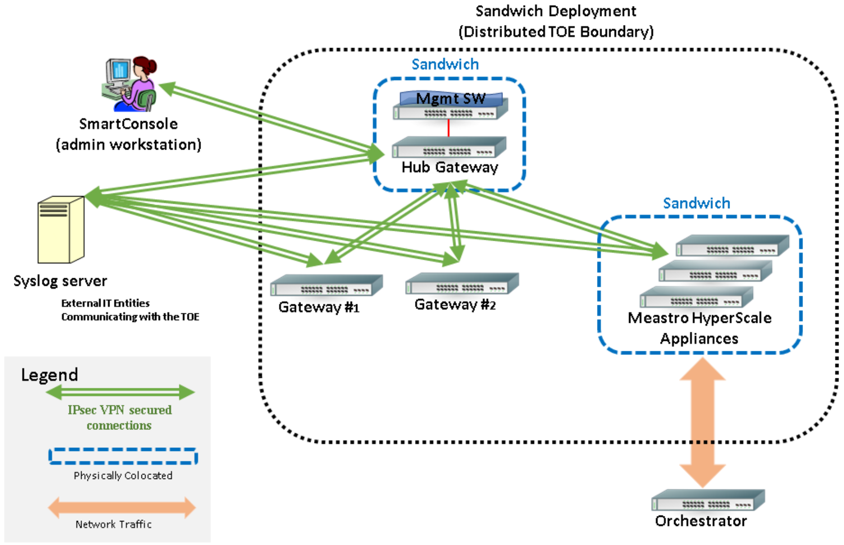
3.2 TOE Architecture

The TOE consists of a family of network appliances whose primary function is to provide firewall capabilities for filtering traffic based on packet rules. As shown in the below figure, the TOE is a distributed system with support for a security management server, allowing remote administration over a protected IPsec connection. The TOE includes the following distributed components:

- a Security Management Server (labelled "Mgmt SW" in the figure below) and
- one or more Check Point Gateway Appliances (Hardware appliances and virtual)

The administrator also uses the SmartConsole Management software client version R81.00 (running on one or more administrative workstations) to manage the system.

All products run Check Point version R81.00 software.



3.3 Physical Boundaries

There are Check Point Security Gateway and Maestro Hyperscale Appliances as well as Security Management Appliances. All platforms use the same image. The difference is mainly in hardware makeup and physical ports. All platforms are x86 based hardware.

The SmartConsole Management GUI software is installed on a Windows workstation (Windows 10 Enterprise). Authorized administrators use the GUI software or CLI to remotely manage the TOE.

The TOE may be configured to interact with an external syslog server. The Orchestrator (as seen in the figure in Section 3.2) provides load balancing between the Maestro gateways; however, the Orchestrator was not evaluated and no claims are made with respect to its functionality.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. User data protection
5. Stateful Traffic Filtering Firewall

6. Identification and authentication
7. Security management
8. Packet filtering
9. Protection of the TSF
10. TOE access
11. Trusted path/channels

4.1 Security audit

The TOE generates audit logs and has the capability to store them internally or to send them to an external audit server. The connection between the TOE and the remote audit server is protected with IPsec. The TOE has a disk cleanup procedure where it removes old audit logs to allow space for new ones. When disk space falls below a predefined threshold (the cleanup procedure cannot keep up with the audit collection), the TOE stops collecting audit records.

4.2 Communication

The TOE is a distributed solution consisting of Security Gateway and Maestro Hyperscale Appliances as well as a Security Management Server. The Security Management Server can manage one or more Security Gateways and Maestro Hyperscale Appliances.

4.3 Cryptographic support

The TOE uses the Check Point Cryptographic Library version 1.1 that has received Cryptographic Algorithm Validation Program (CAVP) certificates for all cryptographic functions claimed in the ST. Cryptographic services include key management, random bit generation, encryption/decryption, digital signature, and secure hashing.

4.4 User data protection

The TOE ensures that residual information is protected from potential reuse in accessible objects such as network packets.

4.5 Stateful Traffic Filtering Firewall

The TOE supports many protocols for packet filtering including icmpv4, icmpv6, ipv4, ipv6, tcp and udp. The firewall rules implement the SPD rules (permit, deny, bypass). Each rule can be configured to log status of packets pertaining to the rule. All codes under each protocol are implemented. The TOE supports FTP for stateful filtering.

Routed packets are forwarded to a TOE interface with the interface's MAC address as the layer-2 destination address. The TOE routes the packets using the presumed destination address in the IP header, in accordance with route tables maintained by the TOE.

IP packets are processed by the Check Point R81.00 software, which associates them with application-level connections, using the IP packet header fields: source and destination IP address and port, as well as IP protocol. Fragmented packets are reassembled before they are processed.

The TOE mediates the information flows according to an administrator-defined policy. Some of the traffic may be either silently dropped or rejected (with notification to the presumed source).

The TOE's firewall and VPN capabilities are controlled by defining an ordered set of rules in the Security Rule Base. The Rule Base specifies what communication will be allowed to pass and what will be blocked. It specifies the source and destination of the communication, what services can be used, at what times, whether to log the connection and the logging level.

4.6 Identification and authentication

The TOE implements a password-based authentication mechanism for authenticating users and requires identification and authentication before allowing access. Only the banner may be presented before authentication is complete. The TOE supports passwords of varying length and allows an administrator to specify a minimum password length between 8 and 100 characters long. The password composition can contain all special characters as required by FIA_PMG_EXT.1.1.

Internally, the TOE keeps track of failed login attempts and if the configured number of attempts is met, the administrator is either locked out for a period of time or until the primary administrator unlocks the account. The local Command Line Interface (CLI) remains available when the remote account is locked out.

The TOE’s IPsec implementation supports Pre-Shared Keys (PSKs) and X.509 certificates (both RSA and ECDSA) for IKE authentication.

4.7 Security management

The TOE allows both local and remote administration for management of the TOE’s security functions. The TOE creates and maintains roles for configured administrators. An administrator can log in locally to the TOE using a serial connection. The local login operates in a CLI. There is one remote administration interface that can be used once the TOE is in its evaluated configuration. The remote administration interface is executed through a Graphical User Interface (GUI) program named SmartConsole using a connection protected by IPsec.

4.8 Packet filtering

Please see the Stateful Traffic Filtering Firewall section for a description of the TOE’s packet filtering mechanism.

4.9 Protection of the TSF

The TOE includes capabilities to protect itself from unwanted modification as well as protecting its persistent data.

The TOE does not store passwords in plaintext; they are obfuscated. The TOE does not support any command line capability to view any cryptographic keys generated or used by the TOE.

The TOE only allows updates after their signature is successfully verified. The TOE update mechanism uses ECDSA with SHA-512 and P-521 to verify the signature of the update package.

The TOE's FIPS executables are signed using ECDSA with SHA-512 and P-521. For all other executables a hash is computed during system installation and configuration and during updates.

During power-up the integrity of all executables is verified. If an integrity test fails in the cryptographic module, the system will enter a kernel panic and will fail to boot. If an integrity test fails due to a non-matching hash, a log is written. Also, during power-up, algorithms are tested in the kernel and user-space. If any of these test fail, the TOE is not operational for users.

The TOE protects all communications among its distributed components with IPsec.

The TOE provides a timestamp for use with audit records, timing elements of cryptographic functions, and inactivity timeouts.

4.10 TOE access

The TOE terminates interactive sessions if the session is inactive for an administrator configured period of time. The TOE also allows a session to be disconnected via a logout command. An administrator can configure a login banner to be displayed before authentication is completed.

4.11 Trusted path/channels

The TOE protects all communications with outside entities using IPsec communications only. The TOE employs IPsec when it sends audit data to an audit server, and when allowing remote administration connections. Any protocol that is part of the distributed TOE must be protected in an IPsec connection.

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020
- *PP-Module for Stateful Traffic Filter Firewalls* for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020
- *PP-Module for Virtual Private Network (VPN) Gateways*, version 1.1, 18 June 2020

That information has not been reproduced here and the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/MOD_VPNGW_v1.1 should be consulted if there is interest in that material.

6 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/MOD_VPNGW_v1.1 and applicable Technical Decisions as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in the *collaborative Protection Profile for Network Devices* with the FW and VPNGW PP-Modules and performed by the Evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

7 Documentation

The following documents were available with the TOE for evaluation:

- *Check Point Software Technologies LTD. Security Gateway Appliances R81.00 Common Criteria Supplement,* Version 1.0, March 16, 2022
- *Check Point Software Technologies LTD. R81.00 NIAP Installation Guide,* Version 1.0, March 16, 2022

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in the proprietary *Detailed Test Report for Check Point Software Technologies Ltd. Security Gateway Appliances R81,* Version 0.3, March 17, 2022 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

8.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/MOD_VPNGW_v1.1 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Security Gateway and Maestro Hyperscale Appliances TOE to be Part 2 extended, and to meet the SARs contained in the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/MOD_VPNGW_v1.1.

9.1 Evaluation of the Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Check Point Security Gateway and Maestro Hyperscale Appliances R81.00 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target and Guidance documents. Additionally, the Evaluation team performed the assurance activities specified in the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/MOD_VPNGW_v1.1 related to the examination of the information contained in the TSS.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guidance was assessed during the design and testing phases of the evaluation to ensure it was complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the cPP_ND_v2.2e/MOD_cPP_FW_v1.4e/ MOD_VPNGW_v1.1 and recorded the results in a Test Report, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the DTR prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The Evaluation team searched the National Vulnerability Database (https://web.nvd.nist.gov/vuln/search), Vulnerability Notes Database (http://www.kb.cert.org/vuls/), Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities), Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories), Exploit / Vulnerability Search Engine (http://www.exploitsearch.net), SecurITeam Exploit Search (http://www.securiteam.com), Tenable Network Security (http://nessus.org/plugins/index.php?view=search), Offensive Security Exploit Database (https://www.exploit-db.com/) on 03/03/2022 with the following search terms: "Check Point", "Gaia", "Firewall", "IPsec", "opsenssl", "ESXI", "Intel Atom Processor C Series", "8th Generation Intel Core i3", "Intel Pentium Gold Processor Series", "Intel Xeon Processor E5 v3 Family", "8th Generation Intel Core i5", "9th Generation Intel Core i9", "Intel Xeon E Processor", "2nd Generation Intel Xeon Scalable", "Xeon E3 Family ", "Intel Pentium Processor D Series", "Intel Celeron Processor 1000 Series".

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the Evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The Validation team suggest that the consumer pay particular attention to the evaluated configuration of the TOE. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 7 to ensure the evaluated configuration is established and maintained. Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00 Security Target*, Version 0.5, March 16, 2022.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.

- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, September 2012.

[2] *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components*, Version 3.1, Revision 5, September 2012.

[3] *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*, Version 3.1 Revision 5, September 2102.

[4] *collaborative Protection Profile for Network Devices*, version 2.2e, 23 March 2020.

[5] *PP-Module for Stateful Traffic Filter Firewalls*, version v1.4 + Errata 20200625, 25 June 2020.

[6] *PP-Module for Virtual Private Network (VPN) Gateways*, version 1.1, 18 June 2020.

[7] *Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00 Security Target*, Version 0.5, March 16, 2022 (ST).

[8] *Assurance Activity Report for Check Point Software Technologies Ltd. Security Gateway and Maestro Hyperscale Appliances R81.00*, Version 0.3, March 17, 2022 (AAR).

[9] *Detailed Test Report for Check Point Security Software Technologies Ltd. Security Gateway Appliances R81*, Version 0.3, March 17, 2022 (DTR).

[10] *Evaluation Technical Report for Check Point Security Gateway and Maestro Hyperscale Appliances*, Version 0.3, March 17, 2022 (ETR)

[11] *Check Point Software Technologies LTD. Security Gateway Appliances R81.00 Common Criteria Supplement*, Version 1.0, March 16, 2022 (AGD)

[12] *Check Point Software Technologies LTD. R81.00 NIAP Installation Guide*, Version 1.0, March 16, 2022