CCEVS APPROVED ASSURANCE CONTINUITY MAINTENANCE REPORT

ASSURANCE CONTINUITY MAINTENANCE REPORT FOR

Quantum Force R81.20

Maintenance Report Number: CCEVS-VR-VID11513-2025

Date of Activity: August 15, 2025

References:

Common Criteria Evaluation and Validation Scheme Publication #6 “Assurance Continuity: Guidance for Maintenance and Re-evaluation” Version 3.0, September 12, 2016

NIAP Policy #12 “Acceptance Requirements of a product for NIAP Evaluation.” 29 August 2014.

Common Criteria document 2012-06-01 “Assurance Continuity: CCRA Requirements” Version 2.1, June 2012

PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.3, 18 August 2023

- Base-PP: collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
- PP-Module: PP-Module for Stateful Traffic Filter Firewalls, Version 1.4e (MOD_CPP_FW_V1.4E)
- PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_V1.3)

Impact Analysis Report for Quantum Force R81.20, Version 1.1, August 14, 2025

Quantum Force R81.20 Security Target, Version 0.4, July 3, 2025

Check Point Software Technologies LTD. Quantum Force R81.20 Common Criteria Supplement, Version 1.1, June 2, 2025

Quantum Force R81.20 NIAP Installation Guide, Version 1.1, June 2, 2025

Affected Evidence:

Quantum Force R81.20 Security Target, version 0.4, 04/23/2025

Check Point Software Technologies LTD. Quantum Force R81.20 Common Criteria Supplement, Version 1.0, April 23, 2025 (CC Guide)

Check Point Software Technologies LTD. Quantum Force R81.20 NIAP Installation Guide, Version 1.0, March 21, 2025 (Install Guide)

Updated Developer Evidence:

This assurance maintenance request is to update the TOE documentation to include 7 new TOE hardware models. The developer has provided sufficient supporting rationale describing the impact of this change. The Security Target, Common Criteria Supplement, and NIAP Installation Guide were updated to include the new TOE models. Additionally, the ST was updated to include a new CAVP certificate to address all cryptographic algorithms for the new TOE models.

Description of Changes:

Gossamer Security Solutions, on behalf of Check Point Software Technologies Ltd., submitted an IAR for approval to update the Quantum Force R81.20 TOE. The TOE was updated to include 7 additional hardware models. An additional CAVP certificate (A4283) was posted to address all cryptographic operations for the new TOE models. As a result, the Security Target, Common Criteria Supplement, and NIAP Installation Guide documents were changed to reflect the new TOE hardware models, and the ST was changed to include reference to the additional CAVP certificate.

Changes to TOE:

The following table presents new hardware models added to the evaluation. Based on the equivalency analysis details in the IAR, all changes are considered **minor**.

#	Product Component CPU	SW Ver	Hardware Models	Network interface
1	I3-13100E (Raptor Lake)	R81.20	9100, 9200	Mgmt, Sync and eth1 through eth8: 1G copper ports based on Intel i210, igb driver
2	I5-13400E (Raptor Cove)	R81.20	9300	Mgmt and Sync: 1G copper ports based on Intel i210, igb driver

#	Product Component CPU	SW Ver	Hardware Models	Network interface
				eth1 through eth8: 1G copper ports based on Intel i350, igb driver
3	I5-13500E (Raptor Cove)	R81.20	9400	Mgmt and Sync: 1G copper ports based on Intel i210, igb driver eth1 through eth4: 10G fiber ports based on Intel x710, i40e driver eth5 through eth12: 1G copper ports based on Intel i350, igb driver
4	Intel 4314 (Ice Lake)	R81.20	9700, 19100	9700 Mgmt and Sync: 1G copper ports based on Intel i210, igb driver eth1 through eth4: 10G fiber ports based on Intel x710, i40e driver eth5 through eth8: 1G copper ports based on Intel i350, igb driver 19100: 2x Mgmt: 10G copper ports based on Intel x550, ixgbe driver 2x Sync: 10G/25G fiber ports based on Intel x710, i40e driver

#	Product Component CPU	SW Ver	Hardware Models	Network interface
5	Intel 4316 (Ice Lake)	R81.20	9800	Mgmt and Sync: 1G copper ports based on Intel i210, igb driver eth1 through eth4: 10G fiber ports based on Intel x710, i40e driver eth5 through eth8: 1G copper ports based on Intel i350, igb driver

The equivalency argument in the IAR was reviewed and it was determined that no additional testing was required for this assurance maintenance. There are no software or operating system changes, and the network drivers for the new models are interfaces already addressed in the original evaluation.

Description of Documentation Changes:

1. Security Target – The Security Target has been updated to identify the new TOE hardware models and new CAVP certificate. No other changes were necessary.
2. Common Criteria Supplement – Common Criteria Supplement was updated to identify the new TOE hardware models. No other changes were necessary to the Common Criteria Supplement.
3. NIAP Installation Guide – NIAP Installation Guide was updated to identify the new TOE hardware models. No other changes were necessary to the NIAP Installation Guide.

Assurance Continuity Maintenance Report:

- Gossamer Security Solutions submitted an Impact Analysis Report (V1.1), on behalf of Check Point Software Technologies Ltd. to update the TOE to include 7 additional TOE models.
- Updates consist of adding the follow models: 9100, 9200, 9300, 9400, 9700, 19100, and 9800.
- These new TOE models warranted an additional CAVP certificate (A4283) to address all cryptographic operation in the ST, which has been posted to the NIST website.
- There are no security relevant updates, so no new certification is required.
- No development environment changes occurred that impacted the product.
- There were no changes that required the evaluators to do any additional testing.

Description of Regression Testing:

Check Point performs regression testing on each product version. This includes low level testing designed to address any CC related issues. Check Point maintains rigorous regression testing protocols

for all modifications integrated into the product. This testing regimen encompasses both security testing and functional testing.

CAVP Analysis:

Algorithm certificate A4283, https://csrc.nist.gov/projects/Cryptographic-Algorithm-Validation-Program/details?source=A&number=4283, has been posted to address all cryptographic operations in the ST. The five product component CPUs for the additional 7 hardware models listed as additions to the evaluation are all included in the new certificate. The CAVP certificate for the evaluated TOE (A2365) still applies.

Vulnerability Assessment:

The public vulnerability search covers the period between the original evaluation search on 4/22/2025 and the updated search performed on 8/14/2025. The evaluator searched the following public vulnerability databases:

- National Vulnerability Database (https://web.nvd.nist.gov/vuln/search, ref NVD)
- Known Vulnerability Exploit Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog, ref KEV)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/, ref VND)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities, ref Rapid7)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories, ref ZDI)
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search, ref TEN)
- Offensive Security Exploit Database (https://www.exploit-db.com/, ref EDB)

with the following search terms:

- "Check Point"
- "CheckPoint"
- "Gaia"
- "ESXi"
- "Firewall"
- "Intel Atom Processor C Series"
- "Intel Pentium Gold Processor Series"
- "Intel 8th Generation Core i3"
- "Intel 8th Generation Core i5"
- "Intel 9th Generation Core i9"
- "Intel Xeon E Processor"
- "Intel 2nd Generation Xeon Scalable"
- "Intel 12th Generation Xeon Scalable"
- "Intel 13th Generation Xeon Scalable"
- "Intel 15th Generation Xeon Scalable"
- "9th Generation Intel Core i5 Processors"
- "13th Generation Intel Core i5 Processors"
- "Intel 3rd Generation Xeon Scalable"

- "Check Point Cryptographic Library"

The IAR contains the output from the vulnerability searches and the rationale why the search results are not applicable to the TOE. No vulnerabilities were discovered that were applicable to the TOE or that were not mitigated or corrected in the TOE via the software minor version update.

Vendor Conclusion:

Hardware platforms have been added to the evaluation scope. The ST has been updated to reflect the new platforms and reference the new Guidance documents. The Guidance documents have been updated with the new platforms.

Note that Check Point continually tracks bugs, vulnerabilities, and other defects reported in the public domain and at the time of this report there are no known outstanding security-related vulnerabilities in the TOE.

Validation Team Conclusion:

The validation team reviewed the changes and concurred the changes are **minor**, and that certificate maintenance is the correct path for assurance continuity as defined in Scheme Process #6. The Security Target, Common Criteria Supplement, and NIAP Installation Guide documents were changed to reflect the new TOE hardware models, and the ST was changed to include reference to the additional CAVP certificate.

Based on this and other information from within the IAR document, the Validation Team agrees that the assurance impact of these changes is **minor**.