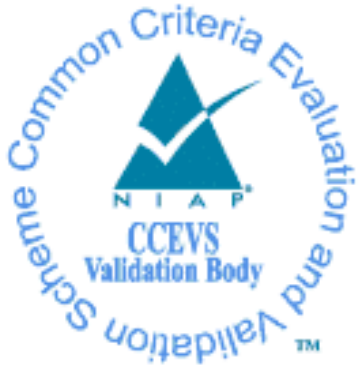
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report
Check Point Software Technologies Ltd. Quantum Force R81.20

Report Number: CCEVS-VR-VID11513-2025
Dated: April 30, 2025
Version: 0.2

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

Jerome Myers, Ph.D.
Meredith Martinez
Seada Mohammed
The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Cummins
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Quantum Force R81.20 solution provided by Check Point Software Technologies Ltd. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation 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 April 2025. 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 PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.3, 18 August 2023 (NDcPP-FW-VPNGW_v1.3) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e) and the PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13).

The Target of Evaluation (TOE) is the Check Point Quantum Force R81.20.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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 Validation Report 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 and the conclusions of the testing laboratory in the evaluation technical report 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 of 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 evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Quantum Force R81.20 Security Target, version 0.4, April 23, 2025 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 Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile 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 Quantum Force R81.20 (Specific models identified in Section 8)
Protection Profile	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.3, 18 August 2023 (NDcPP-FW-VPNGW_v1.3) which includes the Base PP: collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e) and the PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13)
ST	Quantum Force R81.20 Security Target, version 0.4, April 23, 2025
Evaluation Technical Report	Evaluation Technical Report for Quantum Force R81.20, version 0.2, April 23, 2025
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	Jerome Myers, PHD, Meredith Martinez, Seada Mohammed

Item	Identifier

3 Architectural Information

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

The Target of Evaluation (TOE) is Quantum Force Appliances R81.20. The R81.20 version is for enterprise 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 Description

Check Point Gateway appliances provide a broad range of services, features and capabilities. This ST makes a set of claims regarding the product's security functionality, in the context of an evaluated configuration. The claimed security functionality is a subset of the product's full functionality. The evaluated configuration is a subset of the possible configurations of the product, established according to the evaluated configuration guidance.

3.2 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.3 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. 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 R81.20 (running on one or more administrative workstations) to manage the system.

All products either run Check Point version R81.20 software.

The administrator deploys the TOE (as diagrammed in the figure above) with a Security Management Server appliance physically combined with its “Hub” Gateway. Through Hub gateway, the Security Management Server controls other Gateway appliances enrolled into the TOE.

In the evaluated configuration, the administrator co-locates the Security Management Server and its Hub Security Gateway (for example, racked together) and then uses a direct network connection to join the Security Management Server appliance to its Hub Gateway. Once joined in this (or functionally similar) fashion, the administrator then accesses the Security Management Server through its Hub Gateway.

To avoid confusion between Check Point lexicon and that of the NDcPP22e/VPNGW13/STFFW14e protection profiles, the ST refers to the evaluated configuration as a "Sandwich." Thus, an evaluated configuration consists of a Sandwich ("Sandwich") Deployment with an arbitrary number of additional Gateways managed by the Sandwich. The Sandwich deployment qualifies as a distributed TOE and relies upon IPsec VPN connections to secure both Internal (Intra) TOE Transfers and also rely upon IPsec VPN connections to secure both communications with external TOE entities (e.g., a syslog server) and communications with remote administrative sessions.

As mentioned above, all the products run software version R81.20 and the Gateways and Management server use the same image (note that once installed, the Management Server lacks IPsec and Firewall functionality) and contain the same Check Point Cryptographic Library.

Check Point's SmartConsole software (installed on a Windows 10 workstation), while not part of the TOE (i.e., not a TOE component), allows the administrator to remotely manage a deployment. Like a browser, SmartConsole does not enforce any security functions, but instead interacts with the TOE to facilitate remote administration. The administrator can also locally administer each TOE component through access to a Command Line Interface (CLI) over a console connection. The TOE component, Management server and HUB Gateway all offer a CLI.

Check Point R81.20 software is installed on a hardware platform in accordance with TOE guidance, in a FIPS 140 mode. The R81.20 software provides the TOE with storage for an audit trail, an IP stack for in-TOE routing, NIC drivers and an execution environment for daemons and security servers.

Quantum Force appliances mediate information flows between clients and servers located on internal and external networks governed by the firewall. User authentication may be achieved by a remote access client authenticating using IKE, against a certificate. Administrators also need to authenticate to the TOE before they can use the Management GUIs to access Security Management.

Check Point's virtual machine engine supports the definition of separate execution domains for Virtual Systems. Incoming IP packets bind to an appropriate VS corresponding to the logical interface (i.e. physical or virtual LAN interface) on which they are received, and the VS that is defined to receive the packet from that interface. The packets are labeled with the VSID, and are handled in the context of that VS's execution domain, until they are dropped, forwarded out of the gateway, or handed to another VS according to administrator-defined rules.

The product additionally imposes traffic-filtering controls on mediated information flows between clients and servers according to the site's security policy rules. By default, these

security policy rules deny all inbound and outbound information flows through the TOE. Only an authorized administrator has the authority to change the security policy rules.

3.4 Physical Boundaries

The TOE is a distributed TOE consistent with Use Case 3 as defined in the NDcPP22e. There are Quantum Force 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.

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. 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 Quantum Force as well as a Security Management Server. The Security Management Server can manage one or more Quantum Force 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 this 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 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 R81.20 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 CLI remains available when the remote account is locked out.

The TOE's IPsec implementation supports 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 Command Line Interface (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 program named SmartConsole using a connection protected by IPsec.

4.8 Packet filtering

Please see the prior *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 up. 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 is able to terminate 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 & Clarification of Scope

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 (NDcPP22e)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
- PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP22e/STFFW14e/VPNGW13 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/STFFW14e/VPNGW13 as described for this TOE in the Security Target. 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.

Clarification of scope
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 Firewall and VPN Gateway 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.

- Apart from the Admin Guide, additional customer documentation for the specific Network Device, Firewall, VPN models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- 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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/STFFW14e/VPNGW13 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Check Point Software Technologies LTD. Quantum Force R81.20 Common Criteria Supplement, Version 1.0, April 23, 2025
- Check Point Software Technologies LTD. Quantum Force R81.20 NIAP Installation Guide, Version 1.0, March 21, 2025

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 to be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 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 Quantum Force R81.20, Version 0.2, April 23, 2025 (DTR), as summarized in the evaluation Assurance Activity Report for Quantum Force R81.20, Version 0.2, April 23,2025.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/STFFW14e/VPNGW13 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.

8 Evaluated Configuration

Below is a list of hardware platforms included in the evaluation. All platforms are x86 based hardware. These platforms can be installed as a Security Gateway and all are running the R81.20 software. The list also includes a "Smart-1" appliance functioning as a Security Management Server, running the same R81.20 software. Finally, the list includes an ESXi appliance, upon which one can install the R81.20 software either configured as a Security Gateway or as a Security Management Server.

Appliance	CPU	CPU Family
19200	Ice Lake Xeon 2x 4316	Intel Xeon E Processor
29100	Ice Lake Xeon 2x 6330N	Intel® 3rd Generation Xeon® Scalable
29200	Ice Lake Xeon 2x 8358	Intel® 3rd Generation Xeon® Scalable
3600	Denverton C3558	Intel Atom® Processor C Series
3800	Denverton C3758	Intel Atom® Processor C Series
6200	Coffee Lake G5400	Intel® Pentium® Gold Processor Series
6400	Coffee Lake i3-8100	Intel® 8th Generation Core™ i3
6600	Coffee Lake i5-8500	Intel® 8th Generation Core™ i5
6700	Coffee Lake E-2176G	Intel® Xeon® E Processor
6900	Coffee Lake i9-9900 KF	Intel® 9th Generation Core™ i9
7000	Cascade Lake 4216	Intel® 2nd Generation Xeon® Scalable
16200	Cascade Lake Dual Xeon 2x 4214	Intel® 2nd Generation Xeon® Scalable
16600	Cascade Lake Refresh Dual XEON 2x 4214R	Intel® 2nd Generation Xeon® Scalable
26000	Cascade Lake Dual Xeon 2x 5220	Intel® 2nd Generation Xeon® Scalable
28000	Cascade Lake Dual Xeon 2x 6254	Intel® 2nd Generation Xeon® Scalable
28600	Cascade Lake Dual Xeon 2x 6254	Intel® 2nd Generation Xeon® Scalable
QLS250	Cascade Lake Dual Xeon 2x 4214	Intel® 12th Generation Xeon® Scalable
QLS650	Cascade Lake Dual Xeon 2x 5220	Intel® 2nd Generation Xeon® Scalable
Smart-1 600-M	Coffee Lake Xeon: 1x E-2176G	Intel Xeon E Processor
Smart-1 6000-L	Cascade Lake Xeon: 2x 4215R	2nd Generation Intel Xeon Scalable Processors

Smart-1 6000-LS	Cascade Lake Xeon: 2x 6226R	2nd Generation Intel Xeon Scalable Processors
ESXi (HPE ProLiant DL360 Gen10)	Xeon Silver 4214	9th Generation Intel Core i5 Processors

Appliance CPU & CPU Family

The following are the Ethernet controllers used in each evaluated Appliance model.

Appliance	Ethernet Controller
3600 3800	eth5 & Mgmt: Intel Corporation I211 Gigabit Network Connection O\B: Intel Corporation Ethernet Connection X553 1GbE
6200 6400	Intel Corporation I211 Gigabit Network Connection
16200 26000 28000	Intel Corporation I350 Gigabit Network Connection
6600 6700 6900 7000	Mgmt & Sync: Intel Corporation I211 Gigabit Network Connection O\B: Intel Corporation I350 Gigabit Network Connection
16600 28600	Mgmt & Sync: Intel Corporation I350 Gigabit Network Connection O\B: Mellanox Technologies MT27800 Family [ConnectX-5]
Smart-1 600	Ethernet controller: Intel Corporation I350 Gigabit Network Connection
ESXi (HPE ProLiant DL360 Gen10)	Embedded 4 X 1GbE Ethernet Adapter (select models) or HPE FlexibleLOM and optional PCIe stand-up cards, depending on model
QLS250	Built-in dual width card: Mellanox Technologies MT27800 Family [ConnectX-6]
QLS650	O/B eth1 though eth4: Mellanox Technologies MT27800 Family [ConnectX-6]
19200	Mgmt & Sync: Intel Corporation i350 Gigabit Network Connection
29100	1x Built-in dual width card: Mellanox Technologies MT27800 Family [ConnectX-6]
29200	2x 4port 10G cards: Intel Corporation x710 (1/10Gb) Network Connection

Ethernet Controllers

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 Quantum Force R81.20 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/STFFW14e/VPNGW13.

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 Quantum Force R81.20 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 evaluator performed the assurance activities specified in the NDcPP22e/STFFW14e/VPNGW13 related to the examination of the information contained in the TSS.

The validator 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. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator 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 validator 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 NDcPP22e/STFFW14e/VPNGW13 and recorded the results in a Test Report, summarized in the AAR.

The validator 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 Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

On April 22, 2025, the evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) with the following search terms: “Check Point”, “CheckPoint”, “Gaia”, “ESXi”, “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”, “Intel 3rd Generation Xeon Scalable”.

The validator 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 notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this Validation Report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

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.
The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Quantum Force R81.20 Security Target, Version 0.4, April 23, 2025*.

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, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e).

[6] PP-Module for VPN Gateways, Version 1.3, 16 August 2023 (VPNGW13).

[7] Quantum Force R81.20 Security Target, Version 0.4, April 23, 2025 (ST).

[8] Assurance Activity Report for Quantum Force R81.20, Version 0.2, April 23, 2025 (AAR).

[9] Detailed Test Report for Quantum Force R81.20, Version 0.2, April 23, 2025 (DTR).

[10] Evaluation Technical Report for Quantum Force R81.20, Version 0.2, April 23, 2025 (ETR).