National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
FortiGate/FortiOS 6.4

Report Number: CCEVS-VR-11296-2023
Dated: March 9, 2023
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

Lisa Mitchell

Sheldon Durrant

Randy Heimann

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Kevin Steiner

Kenji Yoshino

Wasif Sikder

Conan Hoye

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of FortiGate/FortiOS 6.4 provided by Fortinet, Inc. 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 Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in February 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). 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 (VPN) Gateways, v1.1.

The TOE is FortiGate/FortiOS 6.4. 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 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *FortiGate/FortiOS 6.4 Security Target*, Version 1.2, March 2023, 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 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	FortiGate/FortiOS 6.4
Sponsor and Developer	Fortinet, Inc. 899 Kifer Road Sunnyvale, CA 94086
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, v1.1 • collaborative Protection Profile for Network Devices, v2.2e (CPP_ND) • PP-Module for Stateful Traffic Filter Firewalls, v1.4e (MOD_CPP_FW) • PP-Module for Virtual Private Network (VPN) Gateways, v1.1 (MOD_VPNGW)
ST	*FortiGate/FortiOS 6.4 Security Target*, Version 1.2, March 2023
Evaluation Technical Report	*FortiGate/FortiOS 6.4 Evaluation Technical Report*, Version 1.2, March 2023
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Kevin Steiner, Kenji Yoshino, Wasif Sikder, Conan Hoye
CCEVS Validators	MITRE: Sheldon Durrant, Randy Heimann, Lisa Mitchell, Lori Sarem

3. Architectural Information

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

The TOE is the FortiGate next-generation firewall (NGFW) family of appliances running FortiOS software. The TOE provides high performance, multilayered validated security and granular visibility for end-to-end protection across the entire enterprise.

3.1. TOE Evaluated Configuration

The TOE is FortiGate/FortiOS 6.4 Version 6.4 (FIPS-CC-64-6) running on a physical or virtual device. The physical and virtual devices are listed in Section 3.2.

The TOE contains the following logical interfaces:

- CLI. Administrative CLI via direct serial connection or SSH.
- GUI. Administrative web GUI via HTTPS.
- Remote Logging. Forwarding of TOE audit events to a remote audit server, which is a Fortinet FortiAnalyzer, via TLS.
- VPN Gateway. VPN connections via IPsec.
- WAN/Internet. External IP interface.
- LAN/Internal. Internal IP interface.

Note: FortiAnalyzer is the only remote audit server supported for this evaluation because it supports a TLS channel.

3.2. Physical Boundary

The physical boundary of the TOE includes the FortiGate hardware models shown in Table 2 and the virtual appliances and related hardware shown in Table 3. The virtual appliances are evaluated as virtual Network Devices (vND), which is case 1 of Section 1.2 of NDcPP v2.2e.

Table 2: TOE Hardware Models

Model	CPU	Architecture	RAM	Boot	Storage	ASIC	Entropy	CAVP
FG-61E	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-61F	Fortinet SoC4	ARMv8	2 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FWF-61E	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241

Model	CPU	Architecture	RAM	Boot	Storage	ASIC	Entropy	CAVP
FWF-61F	Fortinet SoC4	ARMv8	2 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-81E	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-81E-PoE	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-81F	Fortinet SoC4	ARMv8	4 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-81F-2R	Fortinet SoC4	ARMv8	4 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-81F-2R-3G4G-PoE	Fortinet SoC4	ARMv8	4 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-81F-2R-PoE	Fortinet SoC4	ARMv8	4 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-81F-PoE	Fortinet SoC4	ARMv8	4 GB	8GB	128GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-90E	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-91E	Fortinet SoC3	ARMv7-A	2 GB	8GB	128GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-101E	Fortinet SoC3	ARMv7-A	4 GB	8GB	480GB	CP9Lite	SoC3	A2225 A2269 A2241
FG-101F	Fortinet SoC4	ARMv8	4 GB	8GB	480GB	CP9XLite	SoC4	A2225 A2269 A2242
FG-201E	Intel Celeron G1820	Haswell	4GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240

Model	CPU	Architecture	RAM	Boot	Storage	ASIC	Entropy	CAVP
FG-201F	Intel Xeon D-1627	Hewitt Lake	8GB	30GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-301E	Intel i5-6500	SkyLake	8GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-401E	Intel i5-8500	Coffee Lake	8GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-501E	Intel i7-6700	SkyLake	16GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-601E	Intel i7-8700	Coffee Lake	16 GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-1101E	Intel Xeon E-2186G	Coffee Lake	16 GB	16GB	960GB	CP9	CP9	A2225 A2269 A2240
FG-1801F	Intel Xeon W-3223	Cascade Lake	24GB	30GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-1801F-DC	Intel Xeon W-3223	Cascade Lake	24GB	30GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-2000E	Intel Xeon E5-1660v4	Broadwell	32 GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-2201E	Intel Xeon Gold 6126	SkyLake	24 GB	16GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-2500E	Intel Xeon E5-1650v3	Haswell	32 GB	16GB	480GB	CP9	CP9	A2225 A2269 A2240
FG-2601F	Intel Xeon Gold 6208U	Cascade Lake	48 GB	30 GB	2 TB	CP9	CP9	A2225 A2269 A2240
FG-2601F-DC	Intel Xeon Gold 6208U	Cascade Lake	48 GB	30 GB	2 TB	CP9	CP9	A2225 A2269 A2240

Model	CPU	Architecture	RAM	Boot	Storage	ASIC	Entropy	CAVP
FG-3301E	Intel Xeon Gold 5118	SkyLake	96 GB	16GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-3401E	Intel Xeon Gold 6130	SkyLake	96 GB	16GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-3401E-DC	Intel Xeon Gold 6130	SkyLake	96 GB	16GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-3601E	Intel Xeon Gold 6152	SkyLake	96 GB	16GB	2TB	CP9	CP9	A2225 A2269 A2240
FG-4201F	Intel Xeon Gold 6248	Cascade Lake	384 GB	30 GB	4 TB	CP9	CP9	A2225 A2269 A2240
FG-4201F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	30 GB	4 TB	CP9	CP9	A2225 A2269 A2240
FG-4401F	Intel Xeon Gold 6248	Cascade Lake	384 GB	30 GB	4 TB	CP9	CP9	A2225 A2269 A2240
FG-4401F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	30 GB	4 TB	CP9	CP9	A2225 A2269 A2240
FG-5001E1	Intel Xeon E5-2690v4	Broadwell	64GB	16GB	480 GB	CP9	CP9	A2225 A2269 A2240
FG-6300F	Intel Xeon D-1567	Broadwell	192GB	16GB	2 TB	CP9	Entropy Token	A2225 A2269 A2240
FG-6301F	Intel Xeon D-1567	Broadwell	192GB	16GB	2 TB	CP9	Entropy Token	A2225 A2269 A2240
FG-6500F	Intel Xeon D-1567	Broadwell	320GB	16GB	2 TB	CP9	Entropy Token	A2225 A2269 A2240
FG-6501F	Intel Xeon D-1567	Broadwell	320GB	16GB	2 TB	CP9	Entropy Token	A2225 A2269 A2240

Table 3: TOE Virtual Appliance and Related Hardware

Model	License	Hypervisor	CPU*	Entropy	CAVP
FortiGate-VM64	VM01 (1x vCPU core and unlimited RAM)	VMware ESXi 6.7	Intel Xeon D-1559 (Broadwell) Intel Xeon E3-1515MV5 (Skylake) Intel Xeon E-2276ME (Coffee Lake)	Token via USB pass-through	A2291 A2298
	VM02 (2x vCPU cores and unlimited RAM)				
	VM04 (4x vCPU cores and unlimited RAM)				
	VM08 (8x vCPU cores and unlimited RAM)				
	VM16 (16x vCPU cores and unlimited RAM)				
	VM32 (32x vCPU cores and unlimited RAM)				
	VMUL (Unlimited vCPU cores and RAM)				

* Provided with PacStar 451/455

3.3. Required Non-TOE Hardware, Software, and Firmware

The TOE operates with the following components in the environment:

- Admin's Workstation. The TOE makes use of a separate workstation for administrative purposes.
- Audit Server. The TOE makes use of a FortiAnalyzer for remote logging.
- VPN Endpoints. The TOE supports FortiGate VPN endpoints.
- CRL Web Server. Web server capable of serving up CRLs over HTTP.
- Hypervisor Environment. The TOE virtual appliances can be deployed to.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. Security Audit

The TOE generates logs for auditable events. These logs can be stored locally in protected storage and/or exported to an external audit server via a secure channel.

4.2. Cryptographic Support

The TOE implements a variety of key generation and cryptographic methods to provide protection of data both in transit and at rest within the TOE. In the evaluated configuration, the TOE is in FIPS mode to support the cryptographic functionality. The TOE implements cryptographic protocols such as SSH, TLS, HTTPS, and IPsec.

4.3. Residual Data Protection

The TOE ensures that data cannot be recovered once deallocated.

4.4. Firewall & Packet Filtering

The TOE allows for the configuration and enforcement of stateful packet filtering/firewall rules on all traffic traversing the TOE.

4.5. Identification and Authentication

The TOE implements mechanisms to ensure that users are both identified and authenticated before any access to TOE functionality or TSF data is granted. Remote login attempts are limited to an administrator-configured threshold, after which the user must wait for a defined period of time before login attempts can be made. It provides the ability to both assign attributes (user names, passwords and roles) and to authenticate users against these attributes. The TOE also provides X.509 certificate validation for its TLS and IPsec connections.

4.6. Security Management

The TOE provides a suite of management functionality, allowing for full configuration of the TOE by an authorized administrator.

4.7. Protection of the TSF

The TOE implements a number of protection mechanisms (including authentication requirements, self-tests and trusted update) to ensure the protection of the TOE and all TSF data. The TOE maintains its own time source free from outside interference for the purpose of generating logs and executing time sensitive operations.

4.8. TOE Access

The TOE provides session management functions for local and remote administrative sections. Administrative sessions have a defined lifetime for both local and remote

sessions, users connecting to the TOE will be presented with a warning and consent banner prior to authentication.

4.9. Trusted Path/Channels

The TOE provides secure channels between itself and local/remote administrators and other devices to ensure data security during transit.

5. Assumptions and 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 (CPP_ND_V2.2e)
- PP-Module for Stateful Traffic Filter Firewalls, v1.4e (MOD_ FW_V1.4e)
- PP-Module for Virtual Private Network (VPN) Gateways, v1.1 (MOD_VPNGW_V1.1)

That information has not been reproduced here and the documents listed above should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2e/MOD_FW_V1.4e/MOD_VPNGW_V1.1 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

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V2.2e, MOD_VPNGW_V1.1 and MOD_FW_V1.4e 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.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 in accordance with the evaluation activities specified in CPP_ND_V2.2-SD, MOD_VPNGW_V1.1-SD and MOD_FW_V1.4e-SD and performed by the Evaluation team
- This evaluation covers only the specific software version 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.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V2.2e, MOD_VPNGW_V1.1 and MOD_FW_v1.4e and applicable Technical Decisions. Any additional security

related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *FortiOS 6.4 and FortiGate NGFW Appliances FIPS 140-2 and NDcPP Common Criteria Technote,* 01-649-0773518-20230309 | March 2023
- *FortiOS 6.4.9 Administration Guide,* Version 6.4.9, 01-649-607590-20220822
- *FortiOS 6.4.9 CLI Reference,* Version 6.4.9, 01-649-684766-20220426
- *FortiOS 6.4.9 Log Reference,* Version 6.4.9, 01-649-619093-20220520
- *FortiOS 6.4 and FortiGate NGFW Appliances, NDcPP Common Criteria Logging Addendum*, 01-649-887811-20230227
- *FortiOS 6.4.0 Hardening your FortiGate,* Version 6.4.0, 01-640-619384-20201210
- *FortiOS 6.4.9 Hardware Acceleration Guide,* Version 6.4.9, 01-649-538746-20230104

All documentation delivered with the product is relevant to and within the scope of the TOE.

7. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *Fortigate/FortiOS 6.4 Assurance Activity Report*, Version 1.2, March 2023 which provides an overview of testing and the prescribed evaluation activities.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Austin, TX and Baltimore, MD from December 2021 until March 2023. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 below.

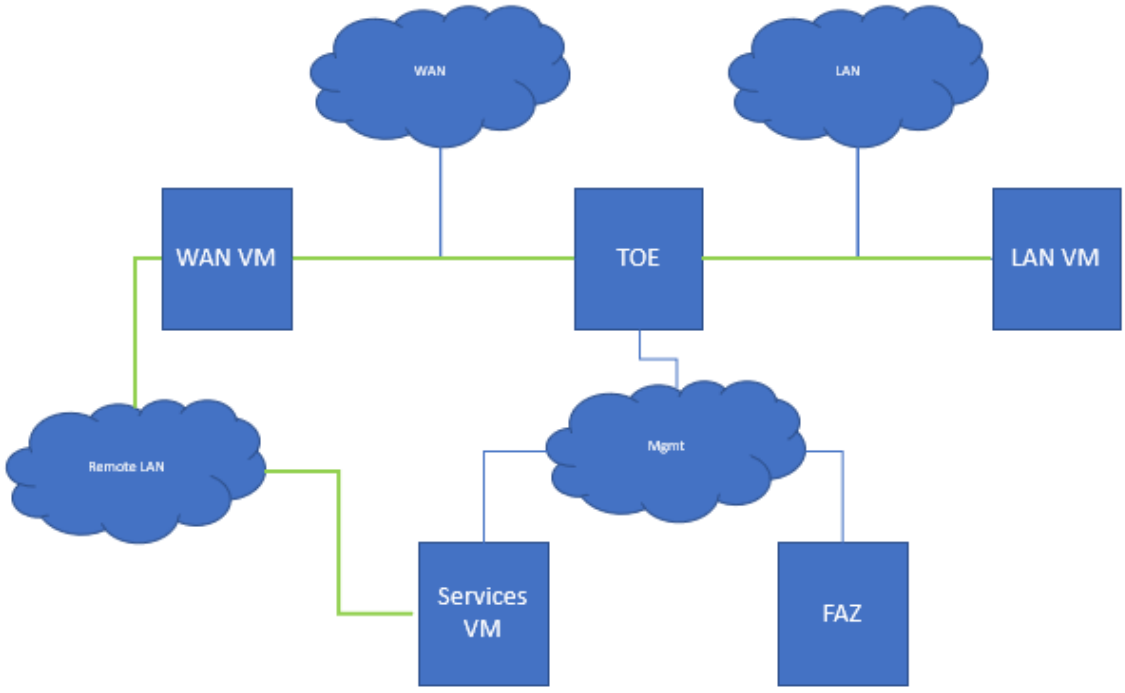

Figure 1: Testing Environment Overview

The green line (——) identifies the path traffic may be routed over. All other connections are for the local subnet.

For IPsec testing, an IPsec tunnel is established between the WAN VM and the TOE.

For a small number of tests (e.g., physical disruption) a dedicated packet capture laptop and traffic mirroring switch were connected directly between the TOE and the rest of the environment.

In summary the evaluator performed full end-to-end testing on the FortiGate VM-64 with VMware ESXi 6.7 and Intel Xeon D-1559 CPU and the FortiGate 2000E models. IPsec was also tested on the FortiGate 81E and 81F.

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all 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 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined FortiGate/FortiOS 6.4 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V2.2-SD, MOD_VPNGW_V1.1-SD and MOD_FW_v1.4e-SD.

8.1. Evaluation of 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 FortiGate/FortiOS 6.4 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.

8.2. Evaluation of Development Documentation (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 ST and Guidance documents. Additionally, the evaluator performed the Evaluation Activities specified in CPP_ND_V2.2-SD, MOD_VPNGW_V1.1-SD and MOD_FW_v1.4e-SD 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 Evaluation Activities and the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3. Evaluation of 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 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.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

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.

8.5. Evaluation of 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 Test Evaluation Activities 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 activities addressed the test activities in CPP_ND_V2.2-SD, MOD_VPNGW_V1.1-SD and MOD_FW_v1.4e-SD and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *FortiGate/FortiOS 6.4 Vulnerability Assessment,* Version 0.4, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on March 2, 2023 did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- US-CERT: http://www.kb.cert.org/vuls/html/search
- Tenable Network Security: https://www.tenable.com/cve
- Tipping Point Zero Day Initiative: https://www.zerodayinitiative.com/advisories
- Offensive Security Exploit Database: https://www.exploit-db.com/
- Rapid7 Vulnerability Database: https://www.rapid7.com/db/vulnerabilities
- Fortinet FortiGuard Services: https://www.fortiguard.com/psirt

The Evaluation team performed a search using the following keywords:

- Each FortiGate hardware and virtual model.
- FortiOS 6.4.9
- Each Processor and Crypto Accelerator used by the TOE.
- OpenSSL 1.1.1q
- OpenSSH 7.1
- TLS
- IPSec
- Fortinet Entropy Token
- Araneus USB TRNG hardware token
- Araneus Alea
- Apache 2.4.41
- Firewall
- TCP, UDP, IPv4, IPv6

When possible, the Evaluation team identified a CPE associated with the search term.

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.

8.7. 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 test activities 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 performed the Evaluation Activities in CPP_ND_V2.2-SD, MOD_VPNGW_V1.1-SD and MOD_FW_v1.4e-SD, and correctly verified that the product meets the claims in the ST.

9. Validator Comments

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.

The Validation team notes that the end user should mitigate the vulnerabilities detailed in CVE-2022-42472 and CVE-2022-39948 by disabling the affected functionality according to guidance provided in *FortiOS 6.4 and FortiGate NGFW Appliances FIPS 140-2 and NDcPP Common Criteria Technote,* 01-649-0773518-20230309 | March 2023 and/or *FortiOS 6.4.9 Administration Guide,* Version 6.4.9, 01-649-607590-20220822 as applicable. Additionally, the end user should update the product when a patch addressing the vulnerabilities is available.

10. Annexes

Not applicable.

11. Security Target

FortiGate/FortiOS 6.4 Security Target, Version 1.2

12. GLOSSARY

- **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.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **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.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
DHCP	Dynamic Host Configuration Protocol
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MFD	Multi-Function Device
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Network Devices,* v2.2E, 23-March-2020
6. *PP-Module for Stateful Traffic Filter Firewalls,* v1.4 + Errata 20200625
7. *PP-Module for Virtual Private Network (VPN) Gateways,* v1.1
8. *FortiGate/FortiOS 6.4 Security Target,* version 1.2
9. *FortiOS 6.4 and FortiGate NGFW Appliances FIPS 140-2 and NDcPP Common Criteria Technote*, 01-649-0773518-20230309 | March 2023
10. *FortiOS 6.4.9 Administration Guide*, Version 6.4.9, 01-649-607590-20220822
11. *FortiOS 6.4.9 CLI Reference,* Version 6.4.9, 01-649-684766-20220426
12. *FortiOS 6.4.9 Log Reference,* Version 6.4.9, 01-649-619093-20220520
13. *FortiOS 6.4 and FortiGate NGFW Appliances, NDcPP Common Criteria Logging Addendum*, 01-649-887811-20230227
14. *FortiOS 6.4.0 Hardening your FortiGate,* Version 6.4.0, 01-640-619384-20201210
15. *FortiOS 6.4.9 Hardware Acceleration Guide,* Version 6.4.9, 01-649-538746-20230104
16. *FortiGate/FortiOS 6.4 Assurance Activity Report*, Version 1.2
17. *FortiGate/FortiOS 6.4 Vulnerability Assessment,* Version 0.4
18. *FortiGate/FortiOS 6.4 Evaluation Technical Report,* Version 1.2
19. *FortiGate/FortiOS 6.4 Detailed Test Report,* Version 1.2
20. *FortiGate/FortiOS 6.4 NDcPPv2.2E Test Plan,* Version 1.1
21. *FortiGate/FortiOS 6.4 MOD_CPP_FW_v1.4e Test Plan,* Version 1.0
22. *FortiGate/FortiOS 6.4 MOD_VPNGWv1.1 Test Plan,* Version 1.0
23. *FortiGate/FortiOS 6.4 FG-2000E NDcPP 2.2E Test Evidence,* Version 1.1
24. *FortiGate/FortiOS 6.4 FG-2000E MOD_VPNGW v1.1 Test Evidence*, Version 1.1
25. *FortiGate/FortiOS 6.4 FG-2000E MOD_CPP_FW_v1.4e Evidence*, Version 1.1
26. *FortiGate/FortiOS 6.4 VM64 NDcPP 2.2E Test Evidence,* Version 0.3
27. *FortiGate/FortiOS 6.4 VM64 MOD_VPNGW v1.1 Test Evidence,* Version 0.4
28. *FortiGate/FortiOS 6.4 FG-VM64 MOD_CPP_FW_v1.4e Evidence*, Version 0.3
29. *FortiGate/FortiOS 6.4 FG-81E MOD_VPNGW v1.1 IPsec Test Evidence*, Version 0.3

30. *FortiGate/FortiOS 6.4 FG-81F MOD_VPNGW v1.1 IPsec Test Evidence*, Version 0.3