National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
FortiGate/FortiOS 7.2

Report Number: CCEVS-VR-VID11562-2025
Dated: October 09, 2025
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

Linda Morrison

Lisa Mitchell

Jenn Dotson

Lori Sarem

Randy Heimann

The MITRE Corporation

Common Criteria Testing Laboratory

Sean Bennett

Nil Folquer

Brandon Solberg

Nathan Bennett

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 7.2 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 October 2025. 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 Gateways*, Version 2.0 and the *Functional Package for Secure Shell (SSH),* Version 1.0.

The TOE is FortiGate/FortiOS 7.2. 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). 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 Security Target 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
Evaluated Product	FortiGate/FortiOS 7.2
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.
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	*PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways*, Version 2.0 (CFG_NDcPP-FW-VPNGW_V2.0) This PP-Configuration includes the following components: i) *Base-PP: collaborative Protection Profile for Network Devices*, Version 3.0e (CPP_ND_V3.0E) ii) *PP-Module: PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4e (MOD_CPP_FW_V1.4E) iii) *PP-Module: PP-Module for VPN Gateways*, Version 1.3 (MOD_VPNGW_V1.3) *Functional Package for Secure Shell (SSH)*, Version 1.0 (PKG_SSH_V1.0)
ST	*FortiGate/FortiOS 7.2 Security Target*, v1.5, October 2025
Evaluation Technical Report	*FortiGate/FortiOS 7.2 Evaluation Technical Report*, v1.3, October 2025
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Sean Bennett, Nil Folquer, Brandon Solberg, Nathan Bennett
CCEVS Validators	The MITRE Corporation

3. Architectural Information

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

FortiGate next-generation firewall (NGFW) appliances running FortiOS software are designed to provide high performance, multilayered security functionality and allows for granular visibility and protection of enterprise network traffic.

3.1. TOE Evaluated Configuration

The TOE is FortiGate/FortiOS 7.2 Version 7.2.8 (FIPS-CC-72-5) running on a physical device. The physical 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.
- CRL. Certificate revocation communication via HTTP.
- NTP Server. Time synchronization via NTP.
- VPN Gateway. VPN connections via IPsec.
- WAN/Internet. External IP interface.
- LAN/Internal. Internal IP interface.

3.2. Physical Boundary

The physical boundary of the TOE includes the FortiGate hardware models shown in Table 2 running FortiOS software identified in Table 1 of the ST.

Table 2: TOE Hardware Models

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-40F	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-40F-3G4G	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FWF-40F	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FWF-40F-3G4G	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-60E	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-60E-PoE	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-60E-DSL	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-60E	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-60E-DSL	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-60E-DSLJ	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-60F	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FGR-60F-3G4G	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FGR-60F	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FWF-60F	Fortinet SoC4	ARMv8	2 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-61E	Fortinet SoC3	ARMv7-A	2 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-61E	Fortinet SoC3	ARMv7-A	2 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-61F	Fortinet SoC4	ARMv8	2 GB	128GB	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FGR-70F	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FGR-70F-3G4G	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-70F	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-71F	Fortinet SoC4	ARMv8	4 GB	128GB	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-80E	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-80E-PoE	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-80F	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-80F-PoE	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FWF-80F-2R	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-81E	Fortinet SoC3	ARMv7-A	2 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-81E-PoE	Fortinet SoC3	ARMv7-A	2 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-81F	Fortinet SoC4	ARMv8	4 GB	128GB	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-81F-PoE	Fortinet SoC4	ARMv8	4 GB	128GB	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FWF-81F-2R	Fortinet SoC4	ARMv8	4 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-81F-2R-3G4G-PoE	Fortinet SoC4	ARMv8	4 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FWF-81F-2R-PoE	Fortinet SoC4	ARMv8	4 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-90E	Fortinet SoC3	ARMv7-A	2 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-91E	Fortinet SoC3	ARMv7-A	2 GB	128GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-100E	Fortinet SoC3	ARMv7-A	4 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-100EF	Fortinet SoC3	ARMv7-A	4 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-100F	Fortinet SoC4	ARMv8	4 GB	N/A	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-101E	Fortinet SoC3	ARMv7-A	4 GB	480GB	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-101F	Fortinet SoC4	ARMv8	4 GB	480GB	CP9XLite	JitterEnt	E139	A2242	A6641	A6643
FG-140E	Fortinet SoC3	ARMv7-A	4 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-140E-PoE	Fortinet SoC3	ARMv7-A	4 GB	N/A	CP9Lite	JitterEnt	E139	A2241	A6641	A6643
FG-200E	Intel Celeron G1820	Haswell	4GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-200F	Intel Xeon D-1627	Hewitt Lake	8GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-201E	Intel Celeron G1820	Haswell	4GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-201F	Intel Xeon D-1627	Hewitt Lake	8GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-300E	Intel Core i5-6500	SkyLake	8GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-301E	Intel Core i5-6500	SkyLake	8GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-400E	Intel Core i5-8500	Coffee Lake	8GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-400F	Intel Xeon E-2336	Cypress Cove (Rocket Lake)	16GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-401E	Intel Core i5-8500	Coffee Lake	8GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-401E-DC	Intel Core i5-8500	Coffee Lake	8GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-401F	Intel Xeon E-2336	Cypress Cove (Rocket Lake)	16GB	960GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-500E	Intel Core i7-6700	SkyLake	16GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-501E	Intel Core i7-6700	SkyLake	16GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-600E	Intel Core i7-8700	Coffee Lake	16 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-600F	Intel Xeon E-	Cypress Cove	16 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
	2386G	(Rocket Lake)								
FG-601E	Intel Core i7-8700	Coffee Lake	16 GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-601F	Intel Xeon E-2386G	Cypress Cove (Rocket Lake)	16 GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-900G	AMD RYZEN 5950E	Zen 3 (Vermeer)	32 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-901G	AMD RYZEN 5950E	Zen 3 (Vermeer)	32 GB	960GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1000F	Intel Xeon E-2388G	Cypress Cove (Rocket Lake)	16GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1001F	Intel Xeon E-2388G	Cypress Cove (Rocket Lake)	16GB	960GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1100E	Intel Xeon E-2186G	Coffee Lake	16 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1100E-DC	Intel Xeon E-2186G	Coffee Lake	16 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-1101E	Intel Xeon E-2186G	Coffee Lake	16 GB	960GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1101E-DC	Intel Xeon E-2186G	Coffee Lake	16 GB	960GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1800F	Intel Xeon W-3223	Cascade Lake	24GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1800F-DC	Intel Xeon W-3223	Cascade Lake	24GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1801F	Intel Xeon W-3223	Cascade Lake	24GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-1801F-DC	Intel Xeon W-3223	Cascade Lake	24GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2000E	Intel Xeon E5-1660 v4	Broadwell	32 GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2200E	Intel Xeon Gold 6126	SkyLake	24 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2201E	Intel Xeon Gold 6126	SkyLake	24 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-2500E	Intel Xeon E5-1650 v3	Haswell	32 GB	480GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2600F	Intel Xeon Gold 6208U	Cascade Lake	48 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2601F	Intel Xeon Gold 6208U	Cascade Lake	48 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-2601F-DC	Intel Xeon Gold 6208U	Cascade Lake	48 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3000F	AMD EPYC 7502P	Zen 2 (Rome)	128 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3000F-DC	AMD EPYC 7502P	Zen 2 (Rome)	128 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3001F	AMD EPYC 7502P	Zen 2 (Rome)	128 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3001F-DC	AMD EPYC 7502P	Zen 2 (Rome)	128 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-3200F	Intel Xeon Gold 6348	Ice Lake	128 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3201F	Intel Xeon Gold 6348	Ice Lake	128 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3300E	Intel Xeon Gold 5118	SkyLake	96 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3301E	Intel Xeon Gold 5118	SkyLake	96 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3400E	Intel Xeon Gold 6130	SkyLake	96 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3400E-DC	Intel Xeon Gold 6130	SkyLake	96 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3401E	Intel Xeon Gold 6130	SkyLake	96 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3401E-DC	Intel Xeon Gold 6130	SkyLake	96 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3500F	AMD EPYC 7542	Zen 2 (Rome)	256 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3501F	AMD EPY	Zen 2 (Rome)	256 GB	4TB	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
	C 7542									
FG-3600E	Intel Xeon Gold 6152	SkyLake	96 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3600E-DC	Intel Xeon Gold 6152	SkyLake	96 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3601E	Intel Xeon Gold 6152	SkyLake	96 GB	2TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3700F	Intel Xeon Gold 6348	Ice Lake	256 GB	4TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3701F	Intel Xeon Gold 6348	Ice Lake	256 GB	4TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3960E	Intel Xeon E5-2650 V4	Broadwell	256 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3960E-DC	Intel Xeon E5-2650 V4	Broadwell	256 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3980E	Intel Xeon E5-2680 V4	Broadwell	256 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-3980E-DC	Intel Xeon E5-	Broadwell	256 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
	2680 V4									
FG-4200F	Intel Xeon Gold 6248	Cascade Lake	384 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4200F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4201F	Intel Xeon Gold 6248	Cascade Lake	384 GB	4 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4201F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	4 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4400F	Intel Xeon Gold 6248	Cascade Lake	384 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4400F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4401F	Intel Xeon Gold 6248	Cascade Lake	384 GB	4 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4401F-DC	Intel Xeon Gold 6248	Cascade Lake	384 GB	4 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-4800F	Intel Xeon Gold 6348	Ice Lake	512 GB	N/A	CP9	JitterEnt	E139	A2240	A6641	A6643

Model	CPU	Architecture	RAM	Storage	ASIC	Entropy	ESV	ASIC CAVP	FortiOS FIPS CAVP	FortiOS SSL CAVP
FG-4801F	Intel Xeon Gold 6348	Ice Lake	512 GB	4 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-5001E1	Intel Xeon E5-2690 v4	Broadwell	64GB	480 GB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-6001F	Intel Xeon D-1567	Broadwell	64GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-6300F	Intel Xeon D-1567	Broadwell	192 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-6301F	Intel Xeon D-1567	Broadwell	192 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-6500F	Intel Xeon D-1567	Broadwell	320 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643
FG-6501F	Intel Xeon D-1567	Broadwell	320 GB	2 TB	CP9	JitterEnt	E139	A2240	A6641	A6643

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.
- NTP Server. The TOE makes use of an NTP server to provide reliable and synchronized time information.

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. User Data Protection

The TOE ensures that residual information and other data cannot be recovered once the associated resource has been deallocated. Data is removed through zeroization.

4.4. Stateful Traffic & 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 supports the use of NTP or its own manually configurable time source free from outside interference for the purpose of generating logs and executing reliable time sensitive operations.

4.8. TOE Access

The TOE provides session management functions for local and remote administrative sessions. 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

The following assumptions are drawn from CPP_ND_V3.0E, PKG_SSH_V1.0, MOD_CPP_FW_V1.4E and MOD_VPNGW_V1.3 as applicable listed here for reader convenience.

Table 3: Assumptions (CPP_ND)

Identifier	Description
A.PHYSICAL_ PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_ FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_ TRAFFIC_ PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

Identifier	Description
A.TRUSTED_ ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_ UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_ CREDENTIALS_ SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_ INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

Table 4: Assumptions (MOD_VPNGW)

Identifier	Description
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

6. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_ND_V3.0E, PKG_SSH_V1.0, MOD_CPP_FW_V1.4E and MOD_VPNGW_V1.3 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 with a certain level of assurance (the assurance activities specified in CPP_ND_V3.0E, PKG_SSH_V1.0, MOD_CPP_FW_V1.4E and MOD_VPNGW_V1.3 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 Firewall, VPN Gateway, Router models was not included in the scope of the evaluation and 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 CPP_ND_V3.0E, PKG_SSH_V1.0, MOD_CPP_FW_V1.4E and MOD_VPNGW_V1.3 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

7. Documentation

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

- *FIPS 140-3 and NDcPP Common Criteria Technote for FortiOS 7.2 and FortiGate NGFW Appliances, 01-728-1075780-20251006, October 6, 2025*
- *FortiOS 7.2.8 Administration Guide, 01-728-791905-20240807, August 7 2024*
- *FortiOS 7.2.8 CLI Reference, 01-728-791773-20240314, March 14 2024*
- *FortiOS 7.2.8 Log Reference, 01-728-791443-20240314, March 14 2024*
- *FortiOS 7.2.8 Hardware Acceleration Guide, 01-729-538746-20240314, March 14 2024*
- *NDcPP Logging Addendum for FortiOS 7.2 and FortiGate NGFW Appliances, 01-728-1172697-20250620, June 20, 2025*
- *FortiOS 6.4.0 Parallel Path Processing, 01-640-619132-20210125, January 25, 2021*

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

8. IT Product Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in *FortiGate/FortiOS 7.2 Assurance Activity Report, version 1.3, October 2025* provides an overview of testing and the prescribed evaluation activities.

8.1. Developer Testing

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

8.2. Evaluation Team Independent Testing

The evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from September 2024 until August 2025. 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.

8.3. Evaluated Configuration

The TOE testing environment components are identified in Figure 1 and 5 below.

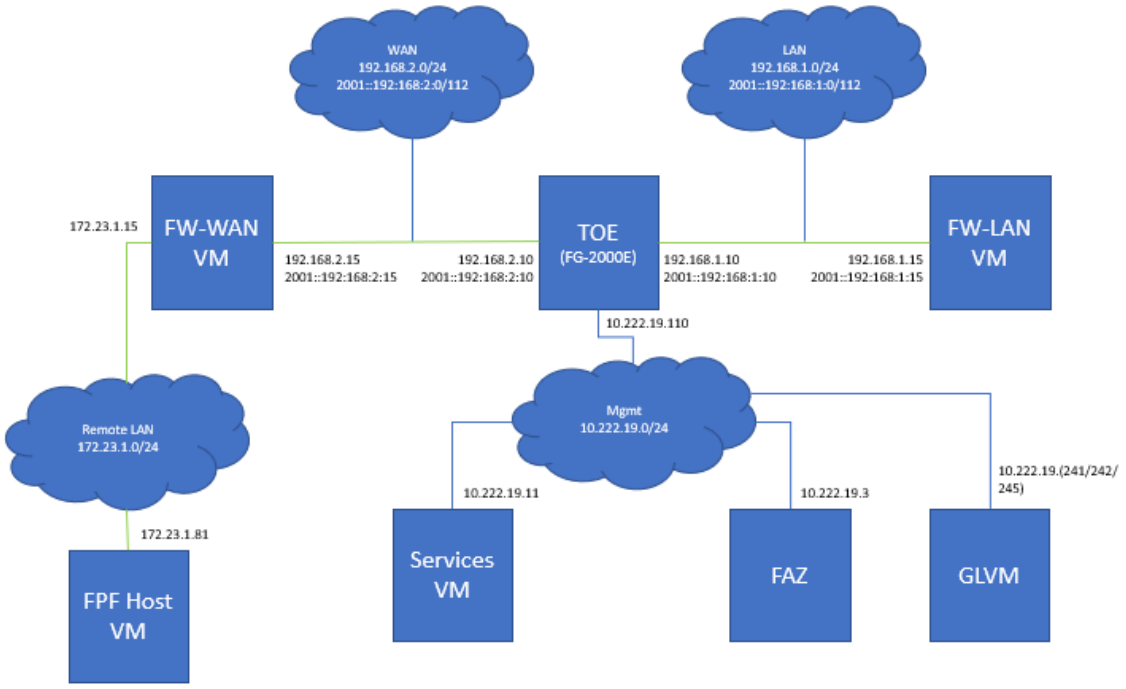

Figure 1: Testing Environment Overview

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 FW-WAN VM and the TOE.

In summary the evaluator performed full end-to-end testing on the FortiGate 2000E and the FortiGate 3001F models. IPsec was also tested on the FortiGate 81E and 81F.

Table 5: Tools Used for Testing

Tool name	Version	Description
Firefox	91.6.0esr	Web Browser for GUI access (evaluator dependent).
Chrome	124.0.6367.61 (Official Build) (64-bit)	Web Browser for GUI access (evaluator dependent).
OpenSSH	8.8p1	SSH server/client
OpenSSL	1.1.1m	General purpose crypto tool
Netcat	1.10-47	TCP/UDP Server/Client
hping3	3.0.0-alpha-2	Arbitrary IPv4 packet creation
sendip	2.6-1	Arbitrary IPv4 & IPv6 packet creation
apache2	2.4.52	HTTP server
Nmap	7.92	Port/Protocol Scanner
Scapy	2.4.5	Send custom packets
Python	3.9.10	Supports Scapy
tcpdump	4.99.1	Packet capture
vsftp	3.0.3-13	FTP server.
Testssl.sh	3.0.8	SSL/TLS Server vulnerability scanner.
Green Light	3.0.54	Custom Lightship Test Tool that performs protocol manipulation and corruption.

Tool name	**Version**	**Description**
		Includes: • Scapy 2.4.5 • Python 3.9.10 • OpenSSH 8.8p1-Lightship-1.1.1 • OpenSSL 1.0.2g-LS 1 Mar 2016
Tool name	**Version**	**Description**
OpenSSH	7.9p1	SSH client for accessing the Remote CLI
OpenSSL	1.1.1n	General purpose crypto tool.
strongSwan	Linux strongSwan U5.7.2/K4.19.0-25-amd64	IPsec peer for NAT testing
dnsmasq	2.80-1	DNS server
syslog-ng	3.19.1-5	Syslog Server
Python	2.7.16	HTTP server
tcpdump	4.9.3	Packet capture
Tool name	**Version**	**Description**
OpenSSH	9.2p1	SSH client for accessing the Remote CLI SSH server/client
OpenSSL	3.0.8	General purpose crypto tool.
Netcat	1.10-41.1	TCP/UDP Server/Client
tcpdump	4.9.3	Packet capture
Python/Python3	3.11.2	TCP/UDP Server
Green Light	3.0.41	Custom Lightship Test Tool that performs protocol manipulation and corruption.

Tool name	Version	Description
		Includes: • Scapy 2.4.4 • Python 3.9.2 • OpenSSH 8.8p1-Lightship-1.0.1 • OpenSSL 1.0.2g-LS 1 Mar 2016
Tool name	**Version**	**Description**
tcpdump	4.9.3	Packet capture
Netcat	1.10-41.1	TCP/UDP Server/Client
OpenSSL	3.0.8	General purpose crypto tool
OpenSSH		SSH client for accessing the Remote CLI SSH server/client
strongSwan	U5.9.8	VPN Peer for FPF testing
Python/Python3	3.11.2	Support Scapy
Scapy	2.5.0	Send custom packets
Green Light	3.0.41	Custom Lightship Test Tool that performs protocol manipulation and corruption. Includes: • Scapy 2.4.4 • Python 3.9.2 • OpenSSH 8.8p1-Lightship-1.0.1 • OpenSSL 1.0.2g-LS 1 Mar 2016

8.4. Excluded Functionality

The following features were not examined as part of this evaluation:

- High-Availability;
- FortiExplorer client;
- FortiGuard Anti-spam, Firmware, Anti-Virus, Content Filtering, Web Filtering, EndPoint Control, and FortiSandbox services;

- Use of syslog;
- FortiToken and FortiSSO Authentication;
- Stream Control Transmission Protocol (SCTP), BGP, RIP, and OSPF protocols;
- Usage of the boot-time configuration menu to upgrade the TOE;
- Policy-based VPN;
- SSL VPN;
- Logging to FortiCloud;
- External Threat Feeds;
- Explicit Web Proxy with Form-Based Authentication;
- REST API;
- Traffic Shaping;
- SMTP;
- SNMP;
- LDAP;
- Windows AD;
- RADIUS;
- USB Interface
- Diagnostics interface;
- DHCP, DDNS, or DNS;
- Traffic offloading to FortiASIC NPx network processors.
- IPS
- HTTP GUI
- Telnet (TOE acting as client or server)
- TFTP (TOE acting as client)
- Precision Time Protocol (PTP)

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 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 7.2 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in both CFG_NDcPP-FW-VPNGW_V2.0 and PKG_SSH_V1.0.

9.1. 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 7.2 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 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 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 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.

9.4. 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.

9.5. 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 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 Fortinet, Inc. FortiGate/FortiOS 7.2 Vulnerability Assessment, v1.0, report prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on October 6, 2025 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
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- 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

The Evaluation team performed a search using the following keywords:

- FortiOS 7.2.8

- FIPS-CC-72
- TOE models
- Each processor and Crypto Accelerator (ASIC) used by the TOE.
- OpenSSL
- OpenSSH
- Apache
- Node.js
- Firewall
- TCP, UDP, IPv4, IPv6, TLS, SSH, IPsec, ICMP, ICMPv6

Note: Additional proprietary search terms were also included.

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 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_V3.0E, PKG_SSH_V1.0, MOD_CPP_FW_V1.4E and MOD_VPNGW_V1.3, and correctly verified that the product meets the claims in the ST.

10. Validator Comments

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *FortiOS 7.2 and FortiGate NGFW Appliances FIPS 140-3 and NDcPP Common Criteria Technote, October 6, 2025*. 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. It is important to note the excluded functionality listed in Section 8.4 and follow any configuration instructions provided to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the CFG_NDcPP-FW-VPNGW_V2.0 and PKG_SSH_V1.0 and accompanying supporting documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11. Annexes

Not applicable.

12. Security Target

Fortinet FortiGate/FortiOS 7.2 Security Target, Version 1.5, October 2025

13. 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.

14. 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

15. Bibliography

The Validation team used the following documents to produce this VR:

[1] *Common Criteria for Information Technology Security Evaluation, Part 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] *PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version: 2.0*

[6] *collaborative Protection Profile for Network Devices, Version 3.0e*

[7] *Evaluation Activities for Network Device cPP, 06-December-2023, Version 3.0e*

[8] *Functional Package for Secure Shell (SSH), Version 1.0*

[9] *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625*

[10] *Supporting Document Mandatory Technical Document Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 +Errata 20200625*

[11] *PP-Module for VPN Gateways, Version 1.3*

[12] *Supporting Document Mandatory Technical Document PP-Module for VPN Gateways, Version: 1.3*

[13] *FortiOS 7.2 and FortiGate NGFW Appliances FIPS 140-3 and NDcPP Common Criteria Technote, October 6, 2025 01-728-1075780-20251006*

[14] *FortiOS 7.2.8 Administration Guide, August 7, 2024 01-728-791905-20240807*

[15] *FortiOS 7.2.8 CLI Reference, March 14, 2024 01-728-791773-20240314*

[16] *FortiOS 7.2.8 Log Reference, March 14, 2024 01-728-791443-20240314*

[17] *FortiOS 7.2 and FortiGate NGFW Appliances NDcPP Common Criteria Logging Addendum, June 20, 2025 01-728-1172697-20250620*

[18] *FortiOS 6.4.0 Parallel Path Processing, January 25, 2021 01-640-619132-20210125*

[19] *FortiOS 7.2.8 Hardware Acceleration, March 14, 2024 01-729-538746-20240314*

[20] *Fortinet FortiGate/FortiOS 7.2 Security Target, v1.5, October 2025*

[21] *FortiGate/FortiOS 7.2 Assurance Activity Report, v1.3, October 2025*

[22] *Fortinet, Inc. FortiGate/FortiOS 7.2 Vulnerability Assessment, v1.2, October 6, 2025*

[23] *FortiGate/FortiOS 7.2 Evaluation Technical Report, v1.3*

[24] *Fortinet, Inc. FortiGate/FortiOS 7.2 Detailed Test Report, v1.2, October 2025*

[25] *Fortinet, Inc. FortiGate/FortiOS 7.2 NDcPPv3.0e + PKG_SSH_V1.0 Test Plan, v1.1, August 2025*
[26] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-2000E NDcPPv3.0e + PKG_SSH_V1.0 Test Evidence, v1.1, October 2025*
[27] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-3001F NDcPPv3.0e + PKG_SSH_V1.0 Test Evidence, v1.1, October 2025*
[28] *Fortinet, Inc. FortiGate/FortiOS 7.2 MOD_CPP_FW_v1.4e Test Plan, v1.0, August 2025*
[29] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-2000E MOD_CPP_FW_v1.4e Evidence, v1.0, August 2025*
[30] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-3001F MOD_CPP_FW_v1.4e Evidence, v1.0, August 2025*
[31] *Fortinet, Inc. FortiGate/FortiOS 7.2 MOD_VPNGWv1.3 Test Plan, v1.0, August 2025*
[32] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-2000E MOD_VPNGWv1.3 Test Evidence, v1.0, August 2025*
[33] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-3001F MOD_VPNGWv1.3 Test Evidence, v1.0, August 2025*
[34] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-81E MOD_VPNGWv1.3 Test Evidence, v1.0, August 2025*
[35] *Fortinet, Inc. FortiGate/FortiOS 7.2 FG-81F MOD_VPNGWv1.3 Test Evidence, v1.0, August 2025*