Certification Report

FortiOS 6.4.9

Sponsor and developer: ***Fortinet, Inc.***
899 Kifer Road
Sunnyvale, CA 94086
USA

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0587886-CR**

Report version: **1**

Project number: **0587886**

Author(s): **Andy Brown**

Date: **14 August 2023**

Number of pages: **12**

Number of appendices: **0**

TÜVRheinland®
Precisely Right.

CONTENTS

TÜVRheinland®
Precisely Right.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

TÜVRheinland®
Precisely Right.

Recognition of the Certificate

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the FortiOS 6.4.9. The developer of the FortiOS 6.4.9 is Fortinet, Inc. located in Sunnyvale, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE provides firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering to provide network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks.

FortiOS can be deployed on a dedicated FortiGate appliance or as a virtual machine running on VMware ESXi. Administration of the system may be performed locally using an administrator console, or remotely via a network management workstation. FortiOS firewalls can operate either standalone or as part of a cluster in order to provide high availability of services.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft. The evaluation was completed on 14-08-2023 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the FortiOS 6.4.9, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the FortiOS 6.4.9 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 Systematic Flaw Remediation

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. Note that the certification results apply only to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the FortiOS 6.4.9 from Fortinet, Inc. located in Sunnyvale, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	FortiOS 6.4.9	FortiOS v6.4.9, FIPS-CC-64-7

To ensure secure usage a set of guidance documents is provided, together with the FortiOS 6.4.9. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE has the following features:

- Security Audit:
  - The TOE creates audit records for administrative events, potential policy violations and information flow decisions. The TOE records the identity of the administrator or user who caused the event for which the audit record is created. The TOE applies timestamps to auditable events as they occur.
- Cryptographic support:
  - Cryptographic functionality is provided to protect communications for remote administration, VPN, and peer-to-peer connections within a cluster.
- User Data Protection:
  - The TOE provides interfaces to a defined set of networks and mediates information flow among these networks. The TOE supports firewall and web filtering policies. The security functional policies are implemented as firewall rules. The rules that implement the Firewall SFP have restrictive default values and by default no information is allowed to flow. The Web Filtering SFP has permissive default values, and does not block URLs until specifically identified. Modification of the rules is restricted to an authorized administrator, and an authorized administrator may also specify alternative initial values to override the default values.
- Identification and authentication:
  - In order to protect the TOE data and services, the TOE requires identification and authentication for all administrative access and network user access to specific services. The TOE maintains identity, role/authorization and authentication data to support this functionality. Identification and authentication are always enforced on the serial interface (local console). On the network interfaces identification and authentication is enforced for all administrator access, specific services, and VPN users.
- Security Management
  - Appropriately authorized administrators may manage security function behaviour, users, IPS policies and information flow policies. The TOE immediately enforces the revocation of a user from an administrative access profile. The TOE provides a web-based GUI and a local Console CLI for administrators to manage all of the security functions. An administrator account consists of an administrator’s identification and authentication information, and access profile. The access profile is a set of permissions that determine which functions the administrator is allowed to access.
- Protection of the TSF:
  - The HA feature provides failover protection capability which includes configuration synchronization. The FortiGate units that make up the HA cluster exchange configuration information using a proprietary protocol (FortiGate Clustering Protocol

(FGCP). Before any information is exchanged, members of a HA cluster authenticate using information built into the FortiGate unit at the time of manufacture.

- Trusted Path / Channels:
  - The TOE provides trusted paths and trusted channels, protected by encryption to guard against disclosure and protected by cryptographic signature to detect modifications. The trusted paths and trusted channels are logically distinct from other communication paths and provide assured identification of their end points. The trusted paths are used to protect remote administrator authentication and all remote administrator actions.
- Intrusion Prevention
  - The TOE provides an Intrusion Prevention System that examines network traffic arriving on its interfaces for evidence of intrusion attempts. Ingress packets received on a FortiGate interface are passed to the Denial of Service sensors, which determine if it is a valid information request or not. Detection of any potential attack is recorded in the IPS or packet logs. If the packet can pass based on the information flow policy (based on the Fortinet Protection Profile), it is examined against IPS signatures known to indicate potential attacks.
- Anti-Virus
  - The TOE detects and prevents virus attacks contained within information flows which arrive at any of its network interfaces. An authorized administrator may configure the TOE to block and or quarantine a virus which is detected in an information flow.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

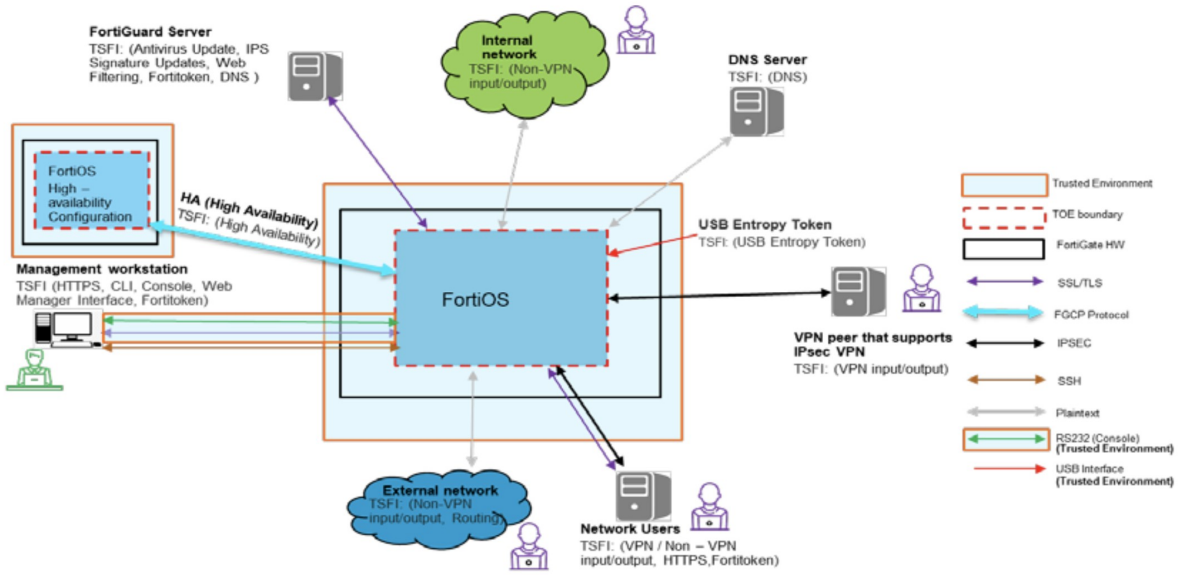
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product

2.4 Architectural Information

The logical architecture of the TOE is depicted below:



FortiOS (TOE) provides firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, antispam protection and content filtering to provide network protection for Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) networks.

FortiOS can be deployed on a dedicated FortiGate appliance or as a virtual machine running on VMware ESXi. Administration of the system may be performed locally using an administrator console, or remotely via a network management workstation. FortiOS firewalls can operate either standalone or as part of a cluster in order to provide high availability of services.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
FortiOS-6.4.9-Administration_Guide	01-649-607590-20220822
FortiOS-6.4.9-CLI_Reference	01-649-684766-20220426
FortiOS_6.4.9_Log_Reference	01-649-619093-20220520
FortiOS – Release Notes	01-649-764531-20220627
FortiOS 6.4 and 7.0 EAL4 Common Criteria Technote	01-649/707-817723-20230718

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

An extensive test execution phase has been performed by the developer. The test information provided described the procedure of executing the tests, test scenarios, non-TOE environment, test coverage and depth correspondence. Test cases covered all TSFI's and all subsystems and module interactions. All [SFR] were tested meaning the complete TSF was also tested.

The evaluator created additional test cases to confirm verification of the version of the TOE / to supplement coverage of SFRs and/or TSFI to further exercise the behaviour of critical functionality.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check were performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS) to collect information about the TOE and identify potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.

The potential vulnerabilities identified were analysed, and some of the potential vulnerabilities were concluded not exploitable or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was two weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator testing and penetration testing was the same as described in the *[ST]*.

2.6.4 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number FortiOS 6.4.9.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the FortiOS 6.4.9, to be **CC Part 2 extended, CC Part 3 conformant** and to meet the requirements of **EAL 4 augmented ALC_FLR.3** .. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the

software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

3 Security Target

The FortiOS® 6.4 Security Target, 01-649-850164-20230718, Version 2.0, 18 July 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
LAN	Local Area Network
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
TOE	Target of Evaluation
VLAN	Virtual LAN

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “Fortinet FortiOS 6.4.x” – EAL4+, 22-RPT-550, 25 July 2023, Version 3.0
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	FortiOS® 6.4 Security Target, 01-649-850164-20230718, Version 2.0, 18 July 2023

(This is the end of this report.)