Certification Report

Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1

Sponsor and developer: ***Cisco Systems, Inc.***
170 West Tasman Drive
95134 San Jose, CA
USA

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

Report number:	**NSCIB-CC-2400046-01-CR**
Report version:	**1**
Project number:	NSCIB-**2400046-01**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**23 March 2025**
Number of pages:	**11**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

CONTENTS

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

Recognition of the Certificate

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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1. The developer of the Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1 is Cisco Systems, Inc. located in San Jose, 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 is a distributed system of multiple components, which together provide firewall and VPN capabilities and centralized management. The TOE is comprised of Cisco Secure Firewall Threat Defense (FTD) software running on Cisco Secure Firewall security appliances that provide the firewall and VPN gateway functionality, and Secure Firewall Management Center (FMC) software running on Cisco Secure FTD appliances that provide centralized management, and the Cisco Secure Client (formerly AnyConnect) providing remote-access.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 23 March 2025 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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1, 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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1 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).

TrustCB 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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1 from Cisco Systems, Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	Cisco Secure Firewall Management Center (FMC)	7.4.2-172
	Cisco Secure Firewall Threat Defense (FTD)	7.4.2-172
	Cisco Secure Client	5.1.2.42

Although the TOE can run on multiple hardware models, the following list of specific hardware models are considered as the non-TOE hardware model in this certification:

Hardware name	Detailed indtentifier
Cisco Secure FTD Appliance	FPR appliances supporting FTD 7.4: • FPR 1000 Series (the same installation and patch files are used for all models in this series: 1010, 1010E, 1120, 1140, and 1150) • Secure Firewall 3100 Series (the same installation and patch files are used for all models in this series: 3105, 3110, 3120, 3130 and 3140) • Secure Firewall 4200 Series (the same installation and patch files are used for all models in this series: 4215, 4225 and 4245)
FMC Appliance	FMC appliances that support FMC 7.4 (the same installation and patch files are used for all hardware models listed here): • FMC 1700 • FMC 2700 • FMC 4700

To ensure secure usage a set of guidance documents is provided, together with the Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE is comprised of several security features including stateful traffic firewall and VPN gateway. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Traffic Flow Control
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

2.3 *Assumptions and Clarification of Scope*

2.3.1 Assumptions

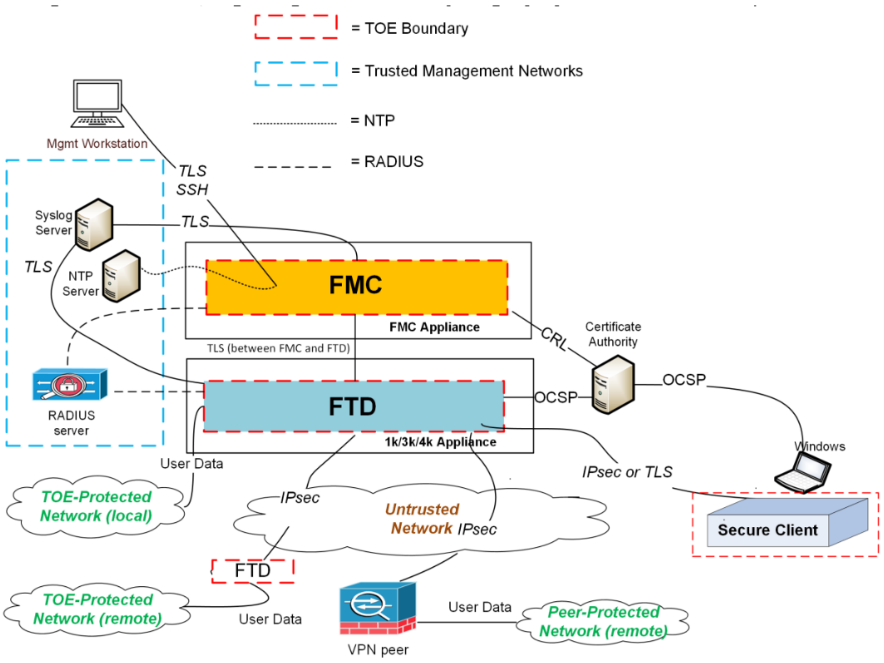
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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 architectureof the TOE can be depicted as follows:



The TOE is a distributed system of multiple components, which together provide firewall and VPN capabilities and centralized management. The TOE is comprised of Cisco Secure Firewall Threat Defense (FTD) software running on Cisco Secure Firewall security appliances that provide the firewall and VPN gateway functionality, and Secure Firewall Management Center (FMC) software running on Cisco Secure FTD appliances that provide centralized management, and the Cisco Secure Client (formerly AnyConnect) providing remote-access.

2.5 *Documentation*

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

Identifier	Version
Cisco Secure Firewall Threat Defense (FTD) 7.4 with FMC and Secure Client Common Criteri Operational User Guidance and Preparative Procedures, version 1.1, Date February 24, 2025	1.1

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

The developer performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

The vulnerability analysis is performed in four parts

- Focused analysis
- CWE Vulnerability focus
- Network scanning tools
- Public domain analysis

A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For all the potential vulnerabilities a penetration test was defined.

The total test effort expended by the evaluators was 2 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The following TOE components was used for testing:

Identifier	Product name	Firmware
FMC	Secure Firewall Management Center	7.4.2-172
FTD	Firewall Threat Defense	7.4.2-172
SC	Secure Client	5.1.2.42

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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1.

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 Cisco Secure Firewall Threat Defense (FTD) 7.4 with Secure Firewall Management Center (FMC) 7.4 and Secure Client 5.1, to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with 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>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Cisco Secure Firewall Threat Defense (FTD) 7.4 with Firewall Management Center (FMC) 7.4 and Secure Client 5.1, v1.1, 24 February 2025 *[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:

ACL	Access Control List
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LAN	Local Area Network
NSCIB	Netherlands Scheme for Certification in the area of IT Security
TOE	Target of Evaluation

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 “Cisco Secure Firewall Threat Defense (FTD) 7.4 with FMC 7.4 and Secure Client 5.1” – EAL4+, 24-RPT-641, Version 4.0, Dated 12 March 2025

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] Cisco Secure Firewall Threat Defense (FTD) 7.4 with Firewall Management Center (FMC) 7.4 and Secure Client 5.1, v1.1, 24 February 2025

(This is the end of this report.)