Certification Report

Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect

Sponsor and developer:	***Cisco Systems, Inc.*** **170 West Tasman Dr.** **San Jose, CA 95134** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-0259553-CR**
Report version:	**1**
Project number:	**0259553**
Author(s):	**Kjartan Jæger Kvassnes**
Date:	**07 October 2022**
Number of pages:	**12**
Number of appendices:	**0**

Head Office:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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, 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.

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

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 Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect. The developer of the Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect 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 software components, which together provide firewall and VPN capabilities and centralized management. The TOE is comprised of Cisco Firepower Threat Defense (FTD) software running on Cisco Firepower security appliances that provide the firewall and VPN gateway functionality, and Firepower Management Center (FMC) software running on Cisco Firepower appliances that provide centralized management, and the AnyConnect Secure Mobility Client providing remote-access VPN functionality.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 22 September 2022 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 Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect, 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 Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect 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.2 (Flaw reporting procedures).

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 Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect from Cisco Systems, Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	FMC	6.4
	FXOS	2.6
	FTD	6.4
	AnyConnect	4.10

To ensure secure usage a set of guidance documents is provided, together with the Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect. 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
  - The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions.
- Traffic Flow Control
  - The TOE provides stateful traffic firewall functionality including IP address-based filtering (for IPv4 and IPv6) to address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance.
- Identification and Authentication
  - The TOE performs multiple types of authentication: device-level authentication of the remote device (VPN peers); authentication of VPN clients (FTD authenticating AnyConnect clients); and user authentication for the authorized administrator of the TOE.
- Security Management
  - The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE.
- Protection of the TSF
  - The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to authorized administrators.
- TOE Access
  - The TOE disconnects sessions that have been idle too long and can be configured to deny sessions based on IP, time, and day, and to NAT external IPs of connecting VPN clients to internal network addresses.

- Trusted Path/Channels
  - The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access, and TLS/HTTPS for GUI access. The TOE supports use of TLS for connections with remote syslog servers (FTD supports syslog over TLS).

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]*.

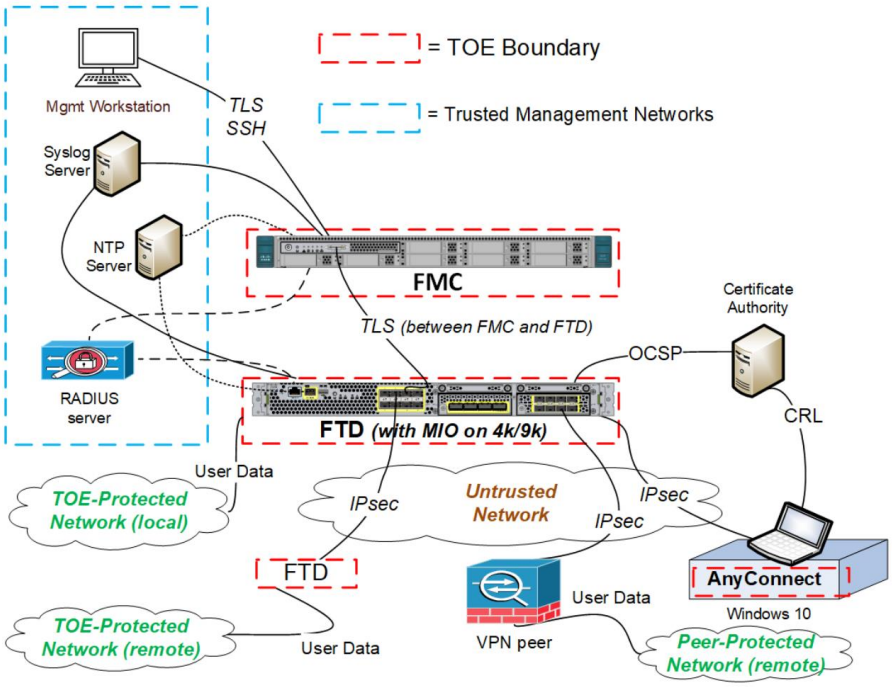
2.3.2 Clarification of scope

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 TOE consists of software images (including operating systems and applications) and a software client application. The TOE includes the Cisco FMC, FTD, MIO, and the Cisco AnyConnect VPN client.

The logical architecture can be depicted as follows:



The figure shown directly above includes the following:

- TOE components: FMC, FTD, MIO, and AnyConnect
- VPN Peer: Another instance of FTD, or a non-TOE peer (Operational Environment)
- Management Workstation (Operational Environment)
- AAA (RADIUS) server (Operational Environment)
- Certificate Authority CA / OCSP Responder (Operational Environment)
- Syslog server (Operational Environment)

- NTP server (Operational Environment)

2.5 Documentation

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

Identifier	Version
Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect Common Criteria Operational User Guidance and Preparative Procedures, dated August 5, 2022	1.0

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

Testing of the Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect is provided by a set of individual test plans. These tests demonstrate the security relevant behaviour of the Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect.

Testing is performed manually and includes both positive and negative testing. Black box testing is performed using the external TSFIs. For the most part, the API interfaces are tested using the corresponding GUI and CLI interfaces that utilize the API. The developer provided a matrix describing the test cases for each TSFI, the corresponding subsystems and modules.

Although the vendor has defined quite a lot of both positive and negative tests for all the TSFIs, the evaluator defined additional independent tests either to cover more scenarios or to gain extra assurance from existing test cases.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- The first step of the vulnerability analysis was the identification of areas of concern (as defined in *[CEM]* and the CWE database, an open source publicly maintained dictionary of software weaknesses).
  - The areas of concern were identified by the evaluator using the CWE generic weaknesses enumeration database version 3.1 as inspiration and the [CEM, Appendix B].
  - Examples of areas of concern are Accessibility, Cryptography, SecureChannel,
- Collecting possible vulnerabilities from the design assessment by posing security questions inspired by generic weaknesses separately for all security implementations of the TOE.
- Collecting possible vulnerabilities from applicable attack lists and public vulnerability search.
- These security relevant questions were then translated into TOE-specific possible vulnerabilities.
- The evaluator determined whether a possible vulnerability was removed or sufficiently mitigated by the TOE implementation/environment evidence. If yes, the possible vulnerability is considered as solved, otherwise it is uniquely labelled as potential vulnerability. Potential vulnerabilities were then addressed in the context of penetration tests and/or further code review.

The total test effort expended by the evaluators was 12 days. 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]*.

The TOE was deployed in an operational environment using the following:

Identifier	Product name	Firmware
FTD[2]	Firepower Threat Defence	6.4.0.15 (on FTD FP 1100) 6.4.0.15 (on FTD FP 2100) 6.4.0.15 (on FTD FP 4100)
FMC	Firepower Management Center	6.4.0.15 (on FMC 4600)
AC	AnyConnect Secure Mobility Client	4.10.05111 (on Windows 10)
FXOS	Firepower Extensible Operating System	2.6.1.254 (on FTD FP 1100) 2.6.1.254 (on FTD FP 2100) 2.6.1.254 (on FTD FP 4100)
MIO[3]	Management Input Output	2.6.1.254

Note: that the ST only claims the first two digits of the software versions, the last two digits only refers to a maintenance release number and a patch build number, respectively.

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

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 Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect. Further details of the TOE components are provided in *[ST]*, chapter 1.3.2 table 3.

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 Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect, to be **CC Part 2 conformant, CC Part 3 conformant**,

[2] Depending on which underlying hardware platforms are used for FTD in the deployed TOE configuration, the deployed TOE will include one or more builds of FXOS. A minimally-featured build of FXOS runs the FTD applications on all platforms (1k, 2k, and on the SM in 4k/9k). A more fully-featured build of FXOS is only present on the 4k/9k platforms and runs in the chassis Supervisor Engine that is not present on the 1k/2k platforms.

[3] To help distinguish between the FXOS builds this document will refer to the FXOS build on the supervisor engine as "MIO" (Management Input/Output), and "FTD" will refer to the FXOS build that loads the FTD applications and also to the FTD applications themselves.

and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. 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 Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect Security Target, Version 1.0, 5 August 2022 *[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:

AC	AnyConnect Secure Mobility Client
CWE	Common Weakness Enumeration
FMC	Firepower Management Center
FTD	Firepower Threat Defense
FXOS	Firepower Extensible Operating System
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MIO	Management Input Output
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
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 Firepower 6.4" – EAL4+, 22-RPT-898, Version 2.0, 24 August 2022
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Cisco Firepower Threat Defense (FTD) 6.4 with FMC and AnyConnect Security Target, Version 1.0, 5 August 2022

(This is the end of this report.)