National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

Validation Report
Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv

Report Number: CCEVS-VR-11290-2023
Dated: January 31, 2023
Version: 0.3

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

Daniel Faigin
Swapna Katikaneni
Deron Graves
Viet Hung Le

The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Kevin Cummins
Douglas Kalmus
Charles Rice
Katie Sykes

Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Gossamer Security Solutions (Gossamer) Common Criteria Testing Laboratory (CCTL) in Columbia, MD, United States of America, and was completed in January 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Gossamer Security Solutions.

The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of the evaluation activities specified in the following materials:

- Base PP: Collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e)
- PP Module for Intrusion Prevention Systems (IPS), Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 18 May 2021
- PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e),
- PP-Module for Virtual Private Network (VPN) Gateways, version 1.0, 18 June 2020 (VPNGW11), and the PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10).

The Target of Evaluation (TOE) is the Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory 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 Validation Report 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 and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing

laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv Security Target, Version 1.1, January 27, 2023 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv (Specific models identified in Section 8)
Protection Profile	Collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e)(PP1) with the PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)(PP-MOD1), the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020

Item	Identifier
	(VPNGW11)(PP-MOD2), and the PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10)(PP-MOD3)
ST	Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv Security Target, Version 1.1, January 27, 2023
Evaluation Technical Report	Evaluation Technical Report for Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv, Version 1.0, January 27, 2023
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 extended
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Daniel Faigin, Swapna Katikaneni, Deron Graves, Viet Hung Le

3 Architectural Information

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

The Cisco Firepower 1000 series and 2100 series are purpose-built, firewall platforms with VPN capabilities and Intrusion Prevention capabilities provided by Firepower Threat Defense (FTD) software. The Firepower Management Center (FMC) physical and virtual appliances provide a centralized management console and event database for the FTD, and aggregates and correlates intrusion, discovery, and connection data from the FTD. In this deployment, the FTD provides VPN, firewall filtering, network analysis, intrusion detection and access control functionalities. The TOE includes one or more FTD appliances that are centrally managed by a Firepower Management Center (FMC) appliance, and together the FMC and FTD appliances form the TOE (Distributed TOE Use Case 3).

3.1 TOE Evaluated Platforms

Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

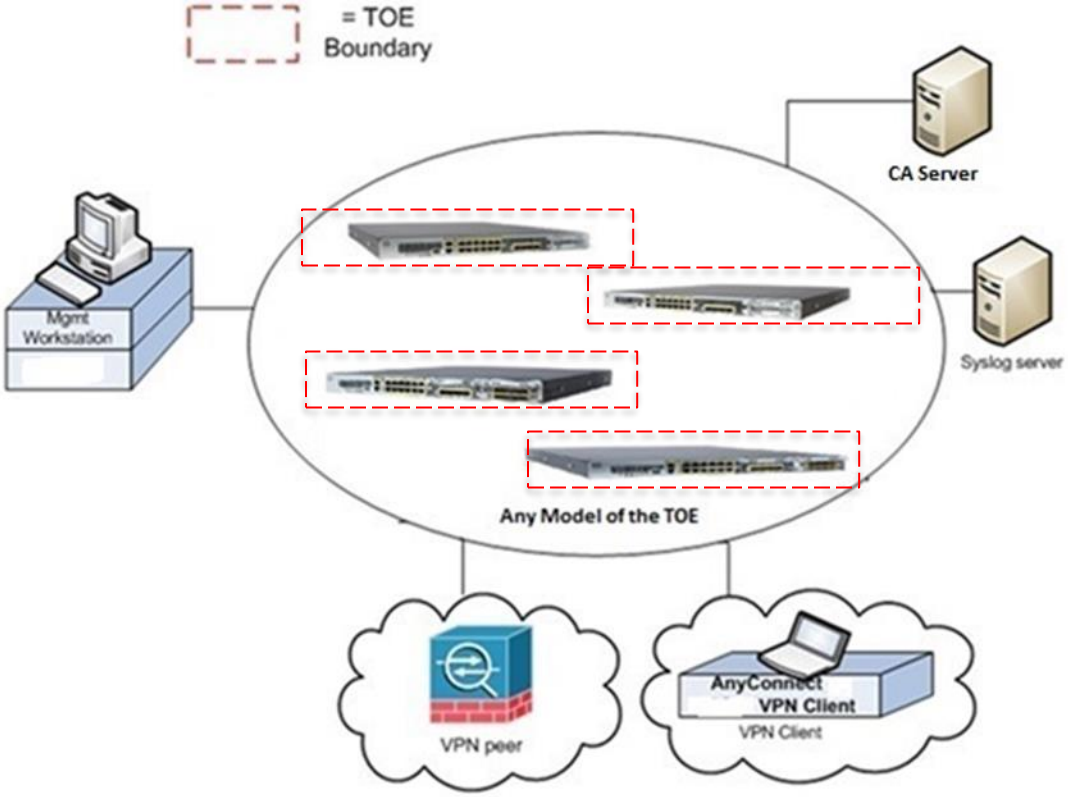
The TOE is comprised of both software and hardware. The TOE appliances are comprised of the following: Firepower 1000 Series (1010, 1120, 1140, 1150), Firepower 2100 Series (2110, 2120, 2130, 2140) and Firepower Management Center (FMC) (FMC1000-K9, FMC2500-K9, FMC4500-K9, FMC1600-K9, FMC2600-K9, FMC4600-K9 and FMCv). The software is comprised of the FTD software image Release 7.0 and FMC (or FMCv) version 7.0.

The models that comprise the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the FTDs in terms of hardware.

The underlying Cisco UCS hardware platforms within the TOE have common hardware characteristics. These differing characteristics affect only non-TSF relevant functionality (such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported, and amount of storage) and therefore support security equivalency of the FMCv in terms of hardware.

3.3 Physical Boundaries

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.



The figure includes the following:

- TOE components (at least one Firepower 2K/1K appliance running FTD v7.0 and FMC/FMCv device running FMC v7.0/FMCv 7.0)
- VPN Peer (Operational Environment) or another instance of the TOE
- VPN Client (Operational Environment) with Cisco AnyConnect Client
- Management Workstation (Operational Environment)
- CA Server (Operational Environment)
- Syslog server (Operational Environment)

4 Security Policy

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

- Security audit
- Communication
- Cryptographic support
- Full residual information protection
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Filtering
- Intrusion Prevention System

4.1 Security audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail where the TOE overwrites the oldest audit record with the newest audit record when space is full. Audit logs are backed up over an encrypted channel to an external audit server.

4.2 Communication

The TOE allows authorized administrators to control which FTD device is managed by the FMC. This is performed through a registration process over TLS. The administrator can also de-register a FTD device if he or she wish to no longer manage it through the FMC.

4.3 Cryptographic support

The TOE provides cryptography in support of other TOE security functionality. The TOE provides cryptography in support of secure connections using IPsec and TLS, and remote administrative management via SSHv2 and TLS/HTTPS. The cryptographic random bit generators (RBGs) are seeded by an entropy noise source.

4.4 Full residual information protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

4.5 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the authorized administrator of the TOE or for IPsec VPN clients. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec X509v3 certificate based authentication or pre-shared key methods while user-level authentication from IPsec VPN clients uses certificate-based authentication (all IPsec VPN sessions are terminated at the FTD, not the FMC/FMCv).

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI and GUI administrator interfaces. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE also implements a lockout mechanism when the number of unsuccessful authentication attempts exceeds the configured threshold.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH and HTTPS interfaces. The SSHv2 interface also supports authentication using SSH keys.

4.6 Security management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 or TLS/HTTPS session, or via a local console connection. Optionally, the FTD component also supports tunneling the SSH connections in IPsec VPN tunnels (peer-to-peer, or remote VPN client). Management of all security functions can be performed via the FMC/FMCv component of the TOE, while a subset of management functions can be performed on the FTD component. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; and the information flow control policies enforced by the TOE including encryption/decryption of information flows for VPNs. The TOE supports an "authorized administrator" role, which equates to any account authenticated to an administrative interface (CLI or GUI, but not VPN), and possessing sufficient privileges to perform security-relevant administrative actions.

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by

the administrator. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

4.7 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and administrator roles to limit configuration to authorized administrators. The TOE prevents reading of cryptographic keys and passwords.

Additionally, the TOE is not a general-purpose operating system and access to the TOE memory space is restricted to only TOE functions.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually via FMC. Additionally, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module. Whenever any system failures occur within the TOE the TOE will cease operation.

4.8 TOE access

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. This is used to provide any information deemed necessary by the administrator. After a configurable period of inactivity, administrator and VPN client sessions will be terminated, requiring re-authentication. The TOE also supports direct connections from VPN clients, and protects against threats related to those client connections. 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.

4.9 Trusted path/channels

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access on the FTD and FMC and TLS/HTTPS for web UI access on the FMC. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec. Note that the VPN client is in the operational environment.

4.10 Filtering

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. Address filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on source and/or destination IP addresses. Port filtering can be configured to restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) and/or receiving (destination) port (service). Stateful packet inspection

is used to aid in the performance of packet flow through the TOE and to ensure that only packets are only forwarded when they're part of a properly established session. The TOE supports protocols that can spawn additional sessions in accordance with the protocol RFCs where a new connection will be implicitly permitted when properly initiated by an explicitly permitted session. The File Transfer Protocol is an example of such a protocol, where a data connection is created as needed in response to an explicitly allowed command connection. System monitoring functionality includes the ability to generate audit messages for any explicitly defined (permitted or denied) traffic flow. TOE administrators have the ability to configure permitted and denied traffic flows, including adjusting the sequence in which flow control rules will be applied, and to apply rules to any network interface of the TOE.

The TOE also provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using VPN policies.

4.11 Intrusion prevention system

The TOE provides intrusion policies consisting of rules and configurations invoked by the access control policy. The intrusion policies are the last line of defense before the traffic is allowed to its destination. All traffic permitted by the access control policy is then inspected by the designated intrusion policy. Using intrusion rules and other preprocessor settings, these policies inspect traffic for security violations and, in inline deployments, can block or alter malicious traffic.

If the vendor-provided intrusion policies do not fully address the security needs of the organization, custom policies can improve the performance of the system in the environment and can provide a focused view of the malicious traffic and policy violations occurring on the network. By creating and tuning custom policies, the administrators can configure, at a very granular level, how the system processes and inspects the traffic on the network for intrusions.

Using Security Intelligence, the administrators can blacklist—deny traffic to and from—specific IP addresses, URLs, and DNS domain names, before the traffic is subjected to analysis by the access control rules. Optionally, the administrators can use a "monitor-only" setting for Security Intelligence filtering.

5 Assumptions & Clarification of Scope

Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e)
- PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e)
- PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020 (VPNGW11)
- PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10)

That information has not been reproduced here and the NDcPP22e/STFFW14e/VPNGW11/IPS10 should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/STFFW14e/VPNGW11/IPS10 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

Clarification of scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 the collaborative Protection Profile for Network Devices with IPS, Firewall, & VPN Gateway 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.
- Additional customer documentation for the specific IPS, Firewall, VPN Gateway models is included in the scope of the evaluation only to the extent it is referenced and used by the Common Criteria specific guidance. Documentation is only included if Validators are instructed to go to those documents and follow specified instructions.
- 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 NDcPP22e/STFFW14e/VPNGW11/IPS10 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco FTD v7.0 on Firepower 1000 and 2100 Series with FMC/FMCv Common Criteria User Guide Supplement IPS & VPN Functionality, Version 1.1, January 27, 2023
- Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC and FMCv Common Criteria Supplemental User Guide, Version 1.1, January 27, 2023
- Cisco Firepower Release Notes, Version 7.0, Last updated: August 10, 2022
- Cisco Firepower Management Center 1000, 2500, and 4500 Hardware Installation Guide, Last updated: August 2018 [FMC-HIG1]
- Cisco Firepower Management Center 1600, 2600, and 4600 Hardware Installation Guide, Last updated: April 29, 2022 [FMC-HIG2]
- Firepower Management Center Upgrade Guide, Last updated: March 1, 2022 [FMC-UG]
- FMC Getting Started Guides [FMC-GS]
    - Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide, Last updated: June 6, 2022
    - Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide, Last updated: April 6, 2020
    - Cisco Secure Firepower Management Center Virtual Getting Started Guide, Last updated: August 26, 2022
- FTD Getting Started Guides [FTD-GS]
    - Cisco Firepower 2100 Getting Started Guide, Last updated: June 28, 2022
    - Cisco Firepower 1100 Getting Started Guide, Last updated: June 28, 2022
- Firepower Management Center Configuration Guide, Version 7.0, Last updated: August 2, 2022 [FMC-CG]
- Cisco Firepower Threat Defense Command Reference, Last updated: June 6, 2022 [FTD-CLI]
- Cisco Firepower Threat Defense Syslog Messages, Last updated: August 15, 2022 [FTD-SYSLOG]

Online help can be accessed in two ways:

- By selecting Product Support > Select a Product
- Search for the Product

The most up-to-date versions of the documentation can be accessed on the Cisco Support web site (http://www.cisco.com/c/en/us/support/index.html).

Any additional customer documentation provided with the product, or that is available online is included in the scope of the evaluation only to the extent it is referenced and used by the Common Criteria specific guidance. Documentation is only included if Validators are instructed to go to those documents and follow specified instructions.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv, Version 1.0, January 27, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to a Common Criteria Certification document and ran the tests specified in the NDcPP22e/STFFW14e/VPNGW11/IPS10 including the tests associated with optional requirements. The AAR, in sections 1.1 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

8 Evaluated Configuration

The evaluated configuration consists of one or more FTD physical devices running the FTD software and one or more physical FMC devices running the FMC software or virtual devices running FMCv software.

Hardware Models and Specifications

TOE Configuration	Hardware Configurations	Software Version
FP2110 **FP2120** **FP2130** **FP2140**	The Cisco FP2100 provides high-performance firewall and VPN services and 4-12 Gigabit Ethernet interfaces, and support for up to 10,000 VPNs.	FTD v7.0
FP1010 **FP1120** **FP1140** **FP1150**	The Cisco FP1000 provides high-performance firewall and VPN services and support for up to 400 VPNs.	FTD v7.0
FMC1000-K9	See FMC Models table below. The FMC models all run the same software image, but have differing hardware	FMC v7.0

FMC2500-K9 **FMC4500-K9** **FMC1600-K9** **FMC2600-K9** **FMC4600-K9**	characteristics which affect only non-security relevant functionality such as throughput, processing speed, number and type of network connections supported, number of concurrent connections supported and amount of storage.	
FMCv	FMCv running on ESXi 6.7 or 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3	FMCv v7.0

8.1 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Telnet for management purposes	Telnet passes authentication credentials in clear text and is disabled by default.
Firepower Device Manager (FDM)	Firepower Device Manager is a web-based local manager. Use of FDM is beyond the scope of this Common Criteria evaluation.
Filtering of non-IP traffic provided by the EtherType option when configuring information flow policies is excluded from the evaluated configuration	Use of non-IP traffic filtering is beyond the scope of this Common Criteria evaluation.
Smart Call Home. The Smart Call Home feature provides personalized, e-mail-based and web-based notification to customers about critical events involving their individual systems.	Use of Smart Call Home is beyond the scope of this Common Criteria evaluation.
Shell Access	The shell access is only allowed for pre-operational installation, configuration, and

	post-operational maintenance and troubling shooting.
NTP	The TOE does not depend on clock updates from NTP servers.
Timeout Exemption Option	The use of the "Exempt from Browser Session Timeout" setting is not permitted. This allows a user to be exempted from the inactivity timeout feature.
REST API	This feature is not evaluated as part of the evaluation. REST API relies on HTTPS as the underlying communication protocol and can be used to build a management interface. This feature is not tested and is out of scope.
Clustering	This feature is not tested and is out of scope.

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 ETR. The reader of this document can assume that all assurance 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 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/STFFW14e/VPNGW11/IPS10.

9.1 Evaluation of the 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 Cisco FTD (NGFW) 7.0 on Firepower

1000 and 2100 Series with FMC/FMCv products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator 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 the Development (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 Security Target and Guidance documents. Additionally the evaluator performed the assurance activities specified in the NDcPP22e/STFFW14e/VPNGW11/IPS10 related to the examination of the information contained in the TSS.

The validator 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 the 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 validator 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 the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator 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 the 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 assurance activities in the NDcPP22e/STFFW14e/VPNGW11/IPS10 and recorded the results in a Test Report, summarized in the AAR.

The validator 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 Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search) and Vulnerability Notes Database (http://www.kb.cert.org/vuls/) on 01/24/2023 with the following search terms: “ftd 7.0”, “Firepower threat defense”, “cisco ssl fom”, “Cisco Security Crypto”, “Virtual fmc fom”, “Firepower management center”, “Openssh”, “ESXi”, “Intel Atom C3000”, “Intel Xeon D”, “Intel Xeon E5”, “Intel Xeon Silver”, “Intel Xeon Gold”, “Intel Xeon Scalable”, “Firepower 1000”, “Firepower 2100”.

The validator 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 testing 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 correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv Security Target, Version 1.1, January 27, 2023*.

13 Glossary

The following definitions are used throughout this document:

- **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.
- **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.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.

[4] collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e).

[5] PP-Module for Stateful Traffic Filter Firewalls, version 1.4 + Errata 20200625, 25 June 2020 (STFFW14e).

[6] PP-Module for Virtual Private Network (VPN) Gateways, version 1.0, 18 June 2020 (VPNGW11).

[7] PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10).

[8] Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv Security Target, Version 1.1, January 27, 2023 (ST).

[9] Assurance Activity Report for Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv, Version 1.0, January 27, 2023 (AAR).

[10] Detailed Test Report for Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv, Version 1.0, January 27, 2023 (DTR).

[11] Evaluation Technical Report for Cisco FTD (NGFW) 7.0 on Firepower 1000 and 2100 Series with FMC/FMCv, Version 1.0, January 27, 2023 (ETR)