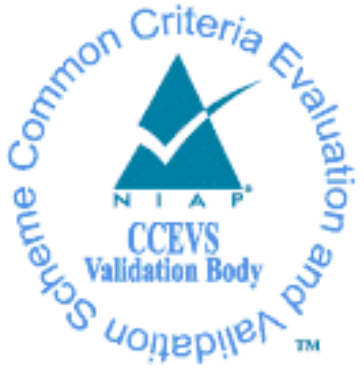
National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme



Validation Report

Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv

Report Number: CCEVS-VR-VID11516-2025
Dated: February 27, 2025
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant
Randy Heimann
Lisa Mitchell
Linda Morrison
Lori Sarem
Chris Thorpe
The MITRE Corporation

Common Criteria Testing Laboratory

Douglas Kalmus
Linh Le
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 7.4 on Firepower 4100 and 9300 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 February 2025. 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 *PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways*, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10), the *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200627, 25 June 2020 (STFFW14e), and the *PP-Module for VPN Gateways*, Version 1.3, 25 August 2023 (VPNGW13).

The Target of Evaluation (TOE) is the Cisco FTD 7.4 on Firepower 4100 and 9300 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 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target*, Version 1.0, February 25, 2025 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 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv (Specific models identified in Section 8)
Protection Profile	*PP-Configuration for Network Devices, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways*, Version 1.2, 18 August 2023 (CFG_NDcPP-IPS-FW-VPNGW_v1.2) which includes the Base PP: *collaborative Protection Profile for Network Devices*, Version 2.2e, 23 March 2020 (NDcPP22e) with the *PP-Module for Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10), the *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200627, 25 June 2020 (STFFW14e), and the *PP-Module for VPN Gateways*, Version 1.3, 25 August 2023 (VPNGW13)
ST	*Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target*, Version 1.0, February 25, 2025
Evaluation Technical Report	*Evaluation Technical Report for Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv*, version 0.2, February 25, 2025
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant

Item	Identifier
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	The MITRE Corporation

3 Architectural Information

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

The Cisco Firepower 4100 and 9300 security appliances are purpose-built, scalable platforms with firewall,VPN and IPS capabilities provided by Firepower Threat Defense (FTD) software that is running on the Firepower eXtensible Operating System (FXOS). The TOE includes one or more Firepower appliances (running FTD and FXOS software) that are centrally managed by a Firepower Management Center (FMC) appliance, and together the FMC and Firepower (running FTD/FXOS) appliances form the TOE (Distributed TOE Use Case 3).

3.1 TOE Description

Each appliance component of the TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

The models that comprise the TOE have common hardware characteristics (for example, the same FXOS image runs on all the models 4100 series and 9300, the same FTD image runs on the FXOS regardless of the platforms and the same FMC image runs on all the FMC appliances). 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 TOE in terms of hardware.

For firewall services, the FTD running on the security module provides application-aware stateful packet filtering firewalls. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The application-inspection capabilities automate the network to treat traffic according to detailed policies based not only on port, state, and addressing information, but also on application information buried deep within the packet header. By comparing this deep-packet inspection information with corporate policies, the firewall will allow or block

certain traffic. For example, it will automatically drop application traffic attempting to gain entry to the network through an open port-even if it appears to be legitimate at the user and connection levels-if a business's corporate policy prohibits that application type from being on the network.

The TOE also provides IPsec connection capabilities. All references within this ST to "VPN" connectivity refer to the use of IPsec tunnels to secure connectivity to and/or from the TOE, for example, gateway-to-gateway[1] VPN or remote access VPN.

The TOE provides intrusion prevention system (IPS) capabilities by combining the security of a Next Generation IPS (NGIPS) with the power of access control, malware protection, and URL/IP filtering known as Security Intelligence. The TOE monitors incoming and outgoing network traffic and performs real-time traffic analysis and logging using the Snort® engine. All packets on the monitored network are scanned, decoded, preprocessed and compared against a set of rules to determine whether inappropriate traffic, such as system attacks, is being sent over the network. The system generates alerts or blocks the traffic when deviations of the expected network behavior are detected or when there is a match to a known attack pattern.

3.2 TOE Evaluated Platforms

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

3.3 TOE Architecture

The TOE is comprised of both software and hardware. The models are comprised of the following: FP 4112, 4115, 4125, 4145 and 9300 and Firepower Management Center (FMC1600, FMC2600, FMC4600, FMC1700, FMC2700, FMC4700 and FMCv). The software is comprised of the FTD software image Release 7.4 (running directly on a 4100 series, or on a security module in a 9300), FXOS 2.14 (running on 4100 series or on the Supervisor blade of a 9300), and FMC (or FMCv) version 7.4.

The Cisco Firepower 9300 security appliance is a modular, scalable, carrier-grade appliance that includes the Chassis (including fans and power supply), Supervisor Blade[2] (to manage the security application running on the security module), network module (optional) and security module that contains the FTD software. The FP4100 Series appliance is a complete standalone, bundle unit that contains everything required above in one appliance.

The Firepower eXtensible Operating System (FXOS) is used to manage the FTD. All the platforms run an instance of FXOS that provides management of the hardware and loads FTD. The 4100/9300 chassis runs on its supervisor engine a fully featured build of FXOS referred to as the Management Input Output (MIO) build of FXOS. A separate, more limited build of FXOS runs on any Security Module (SM) installed within the chassis (the Firepower 4100 models contain one fixed Security Module, while the Firepower 9300 chassis supports up to three removable Security Modules). The SM hardware is a form of

[1] This is also known as site-to-site or peer-to-peer VPN.
[2] Also known as the Cisco FXOS chassis.

Cisco UCS server (based on a UCS B-series blade server), and as such it includes a Cisco Integrated Management Controller (CIMC), which is firmware running on a CIMC daughterboard on the server blade. The FTD software runs on FXOS on the SM. The FXOS software running on the chassis supervisor maintains a list of administrative accounts that are able to log in to the supervisor via CLI or WebUI/GUI, called Firepower Chassis Manager (FCM). All administrative accounts can be managed via both CLI and GUI, and the same authentication mechanisms can be used at the CLI or GUI.

The FMC is a fault-tolerant, purpose-built network appliance that provides a centralized management console and database repository for the Sensors (i.e., FTD). The FMC is a key component in the Cisco NGIPS system. Administrators can use the FMC to manage the full range of Sensors that comprise the Cisco NGIPS system, and to aggregate, analyze, and respond to the threats they detect on their network. By using the FMC to manage Sensors, administrators can:

- Configure policies for all Sensors from a single location, making it easier to change configurations.
- Install various types of software updates on Sensors.
- Push policies to managed Sensors and monitor their health status from the FMC.

The FMC aggregates and correlates intrusion events, anomaly, network discovery information, and Sensor performance data, allowing administrators to monitor the information the Sensors are reporting in relation to one another, and to assess the overall activity occurring on their network. The following illustration lists what is transmitted between a FMC and its managed Sensors.

The UCS hardware components, which provide the platform for the FMCv, in 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.

3.4 Physical Boundaries

The TOE consists of at least one Firepower device (Firepower 4100/9300 series) running the FXOS and FTD software and one physical FMC device running the FMC software or virtual devices running FMCv software. The TOE includes the Cisco FTD, FMC, and FXOS software. Each instantiation of the TOE has two or more network interfaces and is able to filter IP traffic to and through those interfaces.

The TOE can optionally connect to an NTP server via an IPsec tunnel for clock updates. If the TOE is to be remotely administered, the management station must connect using SSHv2. When web UI is used, a remote workstation with a TLS-enabled browser must be available. A syslog server can also be used to store audit records, and the syslog server must support syslog over TLS or IPsec.

FTD supports two different TLS clients that send syslog messages to the external syslog server- FTD TLS client and FTD OS TLS Client. The FTD TLS Client is configured by the

FMC and is the main audit system for audits generated by FTD. It sends audit events such as IPsec and login messages to the external syslog server. Mutual authentication is not supported. The FTD OS TLS client implementation is configured through the FTD's command line and sends audit events such as SSH login, console login, etc. to an external syslog server. Mutual authentication is not supported.

The TOE can filter connections to/from these external entities using its IP traffic filtering, and can encrypt traffic where necessary using TLS, SSH, and/or IPsec. The TOE uses X.509v3 certificates to support authentication for both IPsec and TLS, and the CA server in the Operational environment can be used to obtain digital certificates.

The communication between the FMC software and FTD in Firepower appliance is protected by TLSv1.2. Digital certificates from a CA server are obtained when certificates are used as the authentication method for VPN connection. The TOE protects peer-to-peer VPN connections between itself and VPN peers (connections can be initiated by the TOE or by the peer) using IPsec.

4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. User data protection
5. Identification and authentication
6. Security management
7. Protection of the TSF
8. TOE access
9. Trusted path/channels
10. Filtering
11. 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 an 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 a platform-based entropy noise source.

4.4 User data 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 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 between 1 and 127 characters for FTD, 8 and 127 characters for FMC and FXOS 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 FXOS and FTD support tunneling the SSH and HTTPS connections in IPsec VPN tunnels (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 and FXOS. 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 are used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually via FMC or FXOS or can configure the TOE (FXOS) to use NTP via an IPsec tunnel to synchronize the TOE's clock with an external time source. 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.

The TOE provides the ability to manually upgrade firmware/software for security administrators. Administrators can query the current executing version of the TOE's firmware/software and the most recently installed version via the FMC Web UI.

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 (FMC, FTD, FXOS), and TLS/HTTPS for GUI access (FMC, FXOS). The TOE supports use of TLS and/or IPsec for connections with remote syslog servers and use of IPsec for connections with NTP servers. The TOE can establish trusted paths of peer-to-peer VPN tunnels using IPsec, and VPN client tunnels using IPsec or TLS. 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 Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10)
- *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200627, 25 June 2020 (STFFW14e)
- *PP-Module for VPN Gateways*, Version 1.3, 25 August 2023 (VPNGW13)

That information has not been reproduced here and the NDcPP22e/IPS10/STFFW14e/VPNGW13 should be consulted if there is interest in that material.

Clarification of scope

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e/IPS10/STFFW14e/VPNGW13 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need 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 and the Intrusion Prevention, Firewalls, and VPN Gateways Modules and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific Firewall, VPN Gateway, Router, Intrusion Prevention Systems models was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e/IPS10/STFFW14e/VPNGW13 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 FXOS 2.14 on Firepower 4100/9300 for FTD Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*, Version 1.0, February 25, 2025
- *Cisco FTD v7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Common Criteria Supplemental User Guide*, Version 0.1, February 5, 2025
- *Cisco FTD v7.4 with FMC/FMCv Common Criteria User Guide Supplement IPS & VPN Functionality*, Version 0.4, November 22, 2024

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.

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 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv*, Version 0.2, February 25, 2025 (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/IPS10/STFFW14e/VPNGW13 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 TOE Evaluated Configuration

8.1 Evaluated Configuration

The evaluated configuration includes the following models:

TOE Configuration	Software Version
FP 4112, FP 4115, FP 4125, FP 4145	FXOS release 2.14 and FTD release 7.4
FP 9300	FXOS release 2.14 and FTD release 7.4
FMC1600, FMC2600. FMC4600, FMC1700, FMC2700, FMC4700	FMC release 7.4
FMCv running on ESXi 7.0 on the Unified Computing System (UCS) UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCSC-C220-M6, UCSC-C225-M6, UCSC-C240-M6, UCSC-C220-M7, UCSC-C240-M7and UCS-E1100D-M6	FMCv release 7.4

8.2 Excluded Functionality

The following functionality is excluded from the evaluation.

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.
Root Shell Access	The root shell access is only allowed for pre-operational installation, configuration, and post-operational maintenance and troubling shooting.
Timeout Exemption Option	The use of the “Exempt from Browser Session Timeout” setting is not permitted.

Excluded Functionality	Exclusion Rationale
	This allows a user to be exempted from the inactivity timeout feature.
FXOS REST API	Allows users to programmatically configure and manage their chassis. Use of REST API is beyond the scope of this Common Criteria evaluation.
Clustering	This feature is not tested and is out of scope.

The services in the table above are disabled in the evaluated configuration. Any functionality of the TOE that has not been discussed in Section 6 of this document is not included in the evaluation. The exclusion of this functionality does not affect compliance to collaborative Protection Profile for Network Devices (cpp_nd_v2.2e), PP-Module for Stateful Traffic Filter Firewalls (mod_cpp_fw_v1.4e), PP-Module for Virtual Private Network (VPN) Gateways (mod_vpngw_v1.3) and PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0).

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 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/IPS10/STFFW14e/VPNGW13.

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 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of 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 evaluation team performed the assurance activities specified in the NDcPP22e/IPS10/STFFW14e/ VPNGW13 related to the examination of the information contained in the TSS.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of 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 validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of 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 validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of 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/IPS10/STFFW14e/VPNGW13 and recorded the results in a Test Report, summarized in the AAR.

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluation team searched the following sources:

- National Vulnerability Database (https://web.nvd.nist.gov/view/vuln/search)
- Vulnerability Notes Database (http://www.kb.cert.org/vuls/)
- Rapid7 Vulnerability Database (https://www.rapid7.com/db/vulnerabilities)
- Tipping Point Zero Day Initiative (http://www.zerodayinitiative.com/advisories)
- cve.org CVE Database (https://www.cve.org/),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search)
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The searches were performed on February 7, 2025 with the following search terms: “ftd 7.4”, “FXOS 2.14”, “Firepower threat defense”, “Firepower management center”, “cisco ssl fom”, “Virtual fmc fom”, “Cisco Security Crypto”, “Openssh”, “CiscoSSH”,

"CiscoSSL", "Snort", "ESXi 7.0", "Intel Xeon Bronze", "Intel Xeon Silver", "Intel Xeon Gold", "Intel Xeon Platinum", "Intel Xeon D", "AMD EPYC", "Firepower 3100".

The validation team reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's 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

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *Cisco FXOS 2.14 on Firepower 4100/9300 for FTD Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*, Version 1.0, February 25, 2025, *Cisco FTD v7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Common Criteria Supplemental User Guide*, Version 0.1, February 5, 2025, and the *Cisco FTD v7.4 with FMC/FMCv Common Criteria Supplemental User Guide & VPN Functionality*, Version 0.4, November 22, 2024. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained. It is important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the NDcPP22e/IPS10/STFFW14e/VPNGW13 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target*, Version 1.0, February 25, 2025.

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 VR:

[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 Intrusion Prevention Systems (IPS)*, 1.0, 11 May 2021 (IPS10).

[6] *PP-Module for Stateful Traffic Filter Firewalls*, Version 1.4 + Errata 20200627, 25 June 2020 (STFFW14e).

[7] *PP-Module for VPN Gateways*, Version 1.3, 25 August 2023 (VPNGW13).

[8] *Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Security Target*, Version 1.0, February 25, 2025 (ST).

[9] *Assurance Activity Report for Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv*, Version 0.2, February 25, 2025 (AAR).

[10] *Detailed Test Report for Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv*, Version 0.2, February 25, 2025 (DTR).

[11] *Evaluation Technical Report for Cisco FTD 7.4 on Firepower 4100 and 9300 Series with FMC/FMCv*, Version 0.2, February 25, 2025 (ETR).

[12] *Cisco FXOS 2.14 on Firepower 4100/9300 for FTD Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration*, Version 1.0, February 25, 2025 (FXOS-AGD).

[13] *Cisco FTD v7.4 on Firepower 4100 and 9300 Series with FMC/FMCv Common Criteria Supplemental User Guide*, Version 0.1, February 5, 2025 (FTD-AGD1).

[14] *Cisco FTD v7.4 with FMC/FMCv Common Criteria User Guide Supplement IPS & VPN Functionality*, Version 0.4, November 22, 2024 (FTD-AGD2).