

# National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme



## Validation Report for Cisco NGIPSv 7.0 with FMC/FMCv 7.0

**Report Number:** CCEVS-VR-11339-2023  
**Dated:** May 18, 2023  
**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**

Lauren Brandt  
Randy Heimann  
Lisa Mitchell  
Lori Saren  
Chris Thorpe  
*The MITRE Corporation*

### **Common Criteria Testing Laboratory**

Cody Cummins  
Douglas Kalmus  
*Gossamer Security Solutions, Inc.*  
*Columbia, MD*

## Table of Contents

1	Executive Summary .....	2
2	Identification .....	3
3	Assumptions & Clarification of Scope .....	4
4	Architectural Information .....	5
4.1	TOE Evaluated Platforms .....	5
4.2	TOE Architecture.....	5
4.3	Physical Boundaries.....	6
5	Security Policy .....	6
5.1	Security audit .....	7
5.2	Communication.....	7
5.3	Cryptographic support .....	7
5.4	Identification and authentication.....	7
5.5	Security management.....	7
5.6	Protection of the TSF .....	8
5.7	TOE access.....	8
5.8	Trusted path/channels .....	8
5.9	Intrusion Prevention System.....	8
6	Documentation.....	9
7	Evaluated Configuration .....	9
8	IT Product Testing .....	10
8.1	Developer Testing.....	10
8.2	Evaluation Team Independent Testing .....	10
9	Results of the Evaluation .....	10
9.1	Evaluation of the Security Target (ASE).....	10
9.2	Evaluation of the Development (ADV) .....	10
9.3	Evaluation of the Guidance Documents (AGD) .....	11
9.4	Evaluation of the Life Cycle Support Activities (ALC) .....	11
9.5	Evaluation of the Test Documentation and the Test Activity (ATE) .....	11
9.6	Vulnerability Assessment Activity (VAN).....	11
9.7	Summary of Evaluation Results.....	12
10	Validator Comments/Recommendations .....	12
11	Annexes.....	12
12	Security Target.....	13
13	Glossary .....	13
14	Bibliography .....	13

# 1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco NGIPsv 7.0 with FMC/FMCv 7.0 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 May 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 collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10).

The Target of Evaluation (TOE) is the Cisco NGIPsv 7.0 with FMC/FMCv 7.0.

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 NGIPsv 7.0 with FMC/FMCv 7.0 Security Target, version 1.0, May 16, 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
<b>Evaluation Scheme</b>	United States NIAP Common Criteria Evaluation and Validation Scheme
<b>TOE</b>	Cisco NGIPsv 7.0 with FMC/FMCv 7.0 (Specific models identified in Section 7)
<b>Protection Profile</b>	PP-Configuration for Network Device and Intrusion Prevention Systems (IPS), Version 1.0, 18 May 2021 [base PP: collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (NDcPP22e) with the PP-Module for Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10)]
<b>ST</b>	Cisco NGIPsv 7.0 with FMC/FMCv 7.0 Security Target, version 1.0, May 16, 2023
<b>Evaluation Technical Report</b>	Evaluation Technical Report for Cisco NGIPsv 7.0 with FMC/FMCv 7.0, version 1.1, May 17, 2023
<b>CC Version</b>	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
<b>Conformance Result</b>	CC Part 2 extended, CC Part 3 extended
<b>Sponsor</b>	Cisco Systems, Inc.
<b>Developer</b>	Cisco Systems, Inc.
<b>Common Criteria Testing Lab (CCTL)</b>	Gossamer Security Solutions, Inc. Columbia, MD

Item	Identifier
CCEVS Validators	The MITRE Corporation

### 3 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), version 1.0, 11 May 2021 (IPS10)

That information has not been reproduced here and the NDcPP22e/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/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 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 Network Device, IPS 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 and applicable Technical Decisions.

Any additional security related functional capabilities of the TOE were not covered by this evaluation.

## 4 Architectural Information

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

The TOE, sometimes referred to as Cisco NGIPSv, provides advanced threat protection as an intrusion prevention system that can be deployed inline (as an IPS to block suspicious or malicious traffic in real-time) or passive (as an IPS/IDS sensor) by integrating real-time inspection and logging of IPv4 and IPv6 traffic.

The Firepower Management Center (FMC) is a network appliance that provides a centralized management console and database repository for the Firepower System deployment. Administrators can also deploy 64-bit virtual Firepower Management Centers (FMCv) as ESXi hosts using the VMware vSphere Hypervisor. The FMC is a key component in the Cisco NGIPSv system. Administrators can use the FMC to manage the Cisco NGIPSv system, and to aggregate, analyze, and respond to the threats they detect on their network.

The TOE is an Intrusion Detection and Prevention System, which consists of the FMC and Sensors (Distributed TOE Use Case 3). The FMC provides a centralized management console and event database for the system, and aggregates and correlates intrusion, discovery, and connection data from managed Sensors. Sensors monitor all network traffic for security events and violations and can alert and/or block malicious traffic as defined in the intrusion and access control rules. The TOE in the evaluated configuration deploys at least one FMC managing one or more Sensors. Each model of the TOE consists of a set of appliances or virtual appliances which vary primarily based on the processing power, memory performance, disk space, and port density. The virtual appliances run on hypervisor ESXi and underlying UCS hardware models which also vary based on the processing power, memory performance, disk space, and port density.

### 4.1 TOE Evaluated Platforms

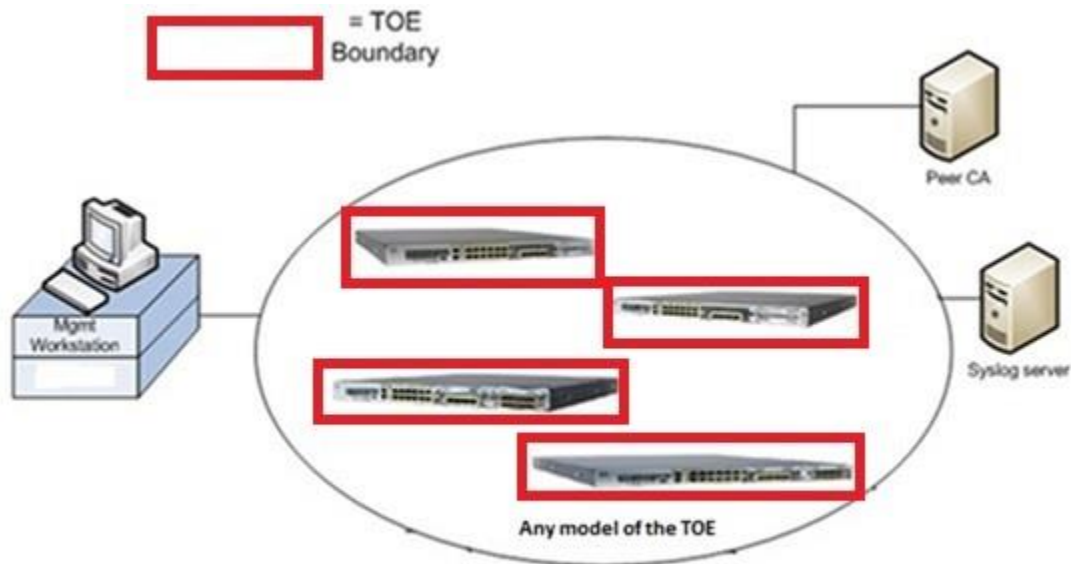
Detail regarding the evaluated configuration is provided in Section 7 below.

### 4.2 TOE Architecture

The TOE combines the security of a Virtual Next Generation Intrusion Prevention System (NGIPSv) 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 industry-leading 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.

### 4.3 Physical Boundaries

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



The previous figure includes the following:

- TOE components (at least one sensor and FMC)
- Management Workstation (Operational Environment)
- Peer CA (Operational Environment)
- Syslog server (Operational Environment)

## 5 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Communication
3. Cryptographic support
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels
9. Intrusion Prevention System



## **5.1 Security audit**

The TOE is designed to be able to generate logs for a wide range of security relevant events such as login attempts and management functions. The TOE can be configured to store the logs locally so they can be accessed by an administrator or alternately to send the logs to an external syslog server over a secure communication channel. The timestamp included in the audit content can be manually set on FMC/FMCv and automatically synchronized with other TOE components.

## **5.2 Communication**

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

## **5.3 Cryptographic support**

The TOE provides FIPS-certified algorithms to provide key management, random bit generation, encryption/decryption, digital signature and secure hashing and key-hashing features in support of higher level cryptographic protocols including TLS, HTTPS, and SSH.

## **5.4 Identification and authentication**

The TOE requires users (i.e., administrators) to be successfully identified and authenticated before they can access any security management functions available in the TOE. The TOE offers both a locally connected console as well as network accessible interfaces (SSHv2 and HTTPS) for remote interactive administrator sessions.

The TOE supports the local (i.e., on device) definition of administrators with usernames and passwords. All authorized TOE users must have a user account with security attributes that control the user's access to TSF data and management functions. These security attributes include username, password, and roles for TOE users. In addition, the TOE supports X.509v3 certificate authentication for the external syslog server.

## **5.5 Security management**

The TOE provides a web-based (using HTTPS) management interface for all TOE administration, including the IDS and access control rule sets, user accounts and roles, and audit functions. The ability to manage various security attributes, system parameters and all TSF data is controlled and limited to those users who have been assigned the appropriate administrative role.

The TOE also provides a command line interface (CLI) and shell access to the underlying operating system of the TOE components. The shell access must be restricted to off-line installation, pre-operational configuration, and maintenance and troubleshooting of the TOE. The CLI provides only a subset of the management functions provided by the web GUI and is only available on the Sensors. The use of the web GUI is highly recommended over the CLI.

Security management relies on a management workstation in the operational environment with a properly supported web browser or SSH client to access the management interfaces.

## **5.6 Protection of the TSF**

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. It protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides its own timing mechanism to ensure that reliable time information is available (e.g., for log accountability) or can utilize a trusted time server in the operational environment.

The TOE ensures that data transmitted between separate parts of the TOE are protected from disclosure or modification. This protection is ensured by transmission of data between the TOE components over a secure, TLS-protected tunnel.

The TOE includes functions to perform self-tests so that it might detect when it is failing. It also includes mechanisms so that the TOE itself can be updated while ensuring that the updates will not introduce malicious or other unexpected changes in the TOE.

## **5.7 TOE access**

The TOE can be configured to display an informative advisory banner when an administrator establishes an interactive session and subsequently enforce an administrator-defined inactivity timeout value after which the inactive session will be terminated. The administrators can also terminate their own interactive sessions when needed.

## **5.8 Trusted path/channels**

The TOE protects interactive communication with administrators using SSHv2 for CLI access or HTTPS for web GUI access. The TOE protects communication with network peers, such as a syslog server, using TLS connections.

## **5.9 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.

## 6 Documentation

The following documents were available with the TOE for evaluation:


- Common Criteria Supplemental User Guide for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.0, May 16, 2023
- Firepower Management Center Configuration Guide, Version 7.0, 2022-09-20
- Cisco Firepower NGIPSv Quick Start Guide for VMware, Version 6.0, November 10, 2015
- Cisco Firepower Release Notes, Version 7.0, 2022-12-19

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 Evaluated Configuration

In the evaluated configuration, the TOE consists of at least one FMC managing one or more Sensors all running version 7.0. The FMC can be a physical appliance or virtual appliance but the sensor is a virtual appliance.

TOE Configuration	Hardware Configuration	Software Version
FMC1000-K9 FMC2500-K9 FMC4500-K9 FMC1600-K9 FMC2600-K9 FMC4600-K9 	The Cisco FMC provides centralized management console with up to 4 management interfaces, and up to 10 Gbps speed.	Release 7.0
FMCv NGIPSv	UCSC-C220-M5, UCSC-C240-M5, UCSC-C480-M5, UCS-E160S-M3 and UCS-E180D-M3 including VM ESXi 6.7 or 7.0	Release 7.0

## 8 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 NGIPsv 7.0 with FMC/FMCv 7.0, Version 1.1, May 17, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

### 8.1 Developer Testing

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

### 8.2 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 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.

## 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 NGIPsv 7.0 with FMC/FMCv 7.0 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e/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 NGIPsv 7.0 with FMC/FMCv 7.0 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 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 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 National Vulnerability Database (<https://web.nvd.nist.gov/view/vuln/search>) and Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>) with the following search terms: “Cisco FirePOWER”, “FMC1600-K9”, “FMCv 7.0”, “NGIPSv”, “VMware v7.0”, “UCSC-C220-M5”, “Intel Xeon Scalable”, “Intel Xeon Skylake”, “Intel Xeon Silver 4110”, “Intel Xeon Silver 4116”, “Intel Xeon E5-2600 v3”, “Intel Xeon E5-2600 v4”, “Intel Xeon D”, “linux-yocto-4.18.45”, “ESXi-7.0”, “OpenSSH 7.6p1”, “OpenSSL”, “CiscoSSL FOM 7.3sp”, “syslog-ng 3.3.2”, “auditd”, “MySQL 15.1”.

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 Common Criteria Supplemental User Guide for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.0 and the supporting documentation listed in the User Guide. This includes instructions for mitigating vulnerabilities as indicated in Section 4.10 of the User Guide. No versions of the TOE and software, either earlier or later, were evaluated.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

It is important to keep in mind, when creating IPS rules, that source or destination IP address entries in Block lists take precedence over those in Do-Not-Block lists. Also, Block and Do-Not-Block rule lists take precedence over intrusion policies.

## 11 Annexes

Not applicable

## 12 Security Target

The Security Target is identified as: *Cisco NGIPSv 7.0 with FMC/FMCv 7.0 Security Target, Version 1.0, May 16, 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 Intrusion Prevention Systems (IPS), version 1.0, 11 May 2021 (IPS10).
- [6] Cisco NGIPSv 7.0 with FMC/FMCv 7.0 Security Target, Version 1.0, May 16, 2023 (ST).
- [7] Assurance Activity Report for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.1, May 17, 2023 (AAR).
- [8] Detailed Test Report for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.1, May 17, 2023 (DTR).
- [9] Evaluation Technical Report for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.1, May 17, 2023 (ETR)
- [10] Common Criteria Supplemental User Guide for Cisco NGIPSv 7.0 with FMC/FMCv 7.0, Version 1.0, May 16, 2023 (CCSUG)
- [11] Firepower Management Center Configuration Guide, Version 7.0, 2022-09-20
- [12] Cisco Firepower NGIPSv Quick Start Guide for VMware, Version 6.0, November 10, 2015
- [13] Cisco Firepower Release Notes, Version 7.0, 2022-12-19