

**National Information Assurance Partnership  
Common Criteria Evaluation and Validation Scheme**



**Validation Report  
Cisco Adaptive Security Appliances (ASA) 9.16 on  
Firepower 1000 and 2100 Series**

**Report Number:** CCEVS-VR-VID11255-2022  
**Dated:** July 15, 2022  
**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**

Patrick Mallett, Ph.D.  
Jerome Myers, Ph.D.  
Elisabeth Scruggs

*The Aerospace Corporation*

### **Common Criteria Testing Laboratory**

Cornelius Haley  
Shahid Islam  
Catherine Sykes  
Douglas Kalmus

*Gossamer Security Solutions, Inc.  
Columbia, MD*

## Table of Contents

1	Executive Summary.....	1
2	Identification.....	1
3	Architectural Information.....	3
3.1	TOE Evaluated Platforms.....	3
3.2	TOE Architecture.....	3
3.3	Physical Boundaries.....	3
4	Security Policy.....	4
4.1	Security audit.....	5
4.2	Cryptographic support.....	5
4.3	Full residual information Protection.....	5
4.4	Identification and authentication.....	5
4.5	Security management.....	5
4.6	Protection of the TSF.....	5
4.7	TOE access.....	6
4.8	Trusted path/channels.....	6
4.9	Filtering.....	6
5	Assumptions & Clarification of Scope.....	7
6	Documentation.....	9
7	IT Product Testing.....	9
7.1	Developer Testing.....	9
7.2	Evaluation Team Independent Testing.....	9
8	Evaluated Configuration.....	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.....	12
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 Adaptive Security Appliances (ASA) Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series 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 (TOE) 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 July 2022. 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 with the collaborative Protection Profile Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020 and the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020.

The TOE is the Cisco Adaptive Security Appliances (ASA) Firepower 1000 and 2100 series device running ASA Version 9.16.

The 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 Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series Security Target, Version 0.5, May 18, 2022, 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 Adaptive Security Appliances (ASA) Firepower 1000 and 2100 series device running ASA Version 9.16 (Specific models identified in Section 8)
<b>Protection Profile</b>	collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 with the collaborative Protection Profile Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020 and the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020
<b>ST</b>	Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series Security Target, Version 0.5, May 18, 2022
<b>Evaluation Technical Report</b>	Evaluation Technical Report for Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series, version 0.2, July 15, 2022
<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
<b>CCEVS Validators</b>	Patrick Mallett, Jerome Myers, Elizabeth Scruggs

### 3 Architectural Information

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

The TOE is comprised of both software and hardware. The hardware models are: Firepower 1000 Series (FP-1010, FP-1120, FP-1140, FP-1150) and 2100 Series (FP-2110, FP-2120, FP-2130, FP-2140). The software is comprised of the Adaptive Security Appliance software image Release 9.16. All of the Firepower 1000 series devices run the same image file. All of the Firepower 2100 Series devices run the same image file.

The Cisco Adaptive Security Appliances 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 ASAs in terms of hardware.

#### 3.1 TOE Evaluated Platforms

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

#### 3.2 TOE Architecture

The TOE is a purpose-built network device with firewall and VPN gateway capabilities. The firewall and VPN Gateway capabilities are as defined in the PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways (CFG\_NDcPP-FW-VPNGW\_V1.1). The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

The TOE protects itself from tampering and bypass by offering only a limited and controlled set of functions at each of its physical interfaces to its environment. Communication via those interfaces is either directed at the TOE for the purpose of administration or is directed through the TOE for communication among network devices. In both cases the TOE implements a set of policies to control the services available and those services are designed to protect and ensure the secure operation of the TOE.

#### 3.3 Physical Boundaries

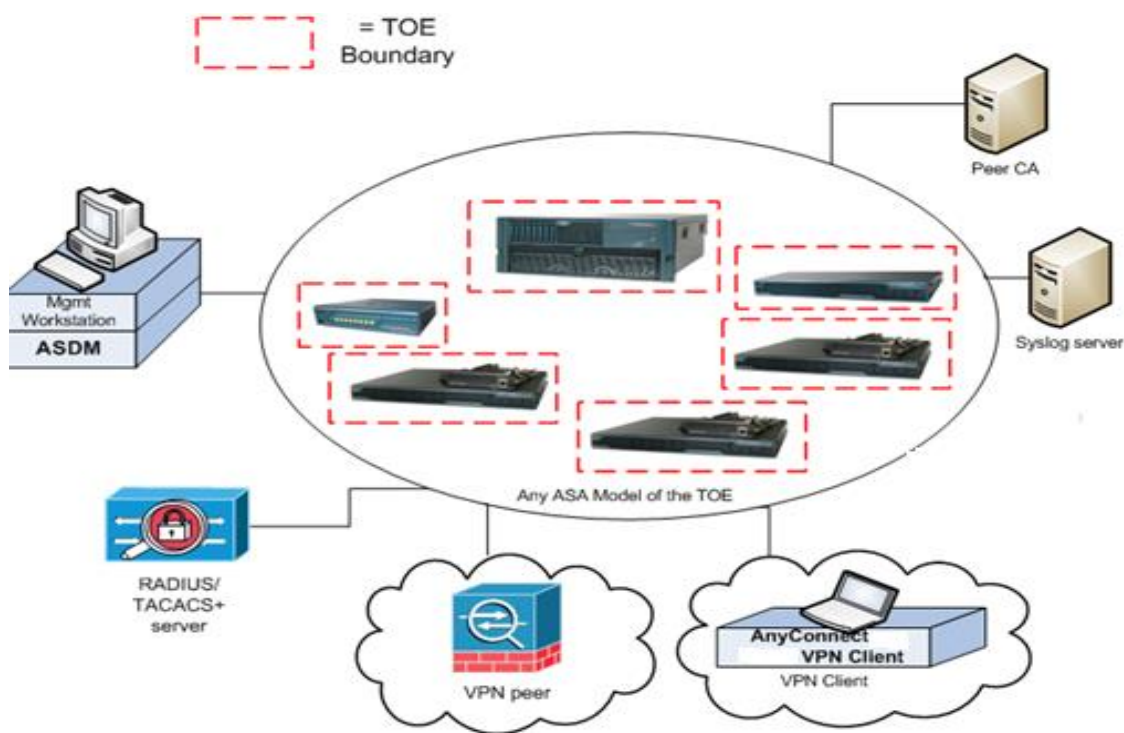
The TOE consists of a physical device as specified below and includes the Cisco ASA software. Each instantiation of the TOE has two or more network interfaces and is able to filter IP traffic to and through those interfaces.

TOE Configuration	Hardware Configurations	Software Version
FP1010 FP1120 FP1140 FP1150	The Cisco ASA Adaptive Security Appliance on FP1000 provides high-performance firewall and VPN services	ASA release 9.16

<b>FP2110</b> <b>FP2120</b> <b>FP2130</b> <b>FP2140</b>	The Cisco ASA Adaptive Security Appliance on FP2100 provides high-performance firewall and VPN services	ASA release 9.16
--	---	------------------

The TOE optionally supports use of AAA server including RADIUS and TACACS+ (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE. The TOE is able to filter connections to/from these external entities using its IP traffic filtering and can encrypt traffic where necessary using TLS and/or IPsec.

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



## 4 Security Policy

This section summarizes the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. Full residual information protection
4. Identification and authentication
5. Security management
6. Protection of the TSF
7. TOE access
8. Trusted path/channels
9. Filtering

## **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 newest audit record will overwrite the oldest audit record when the local storage space for audit data is full. Audit logs are backed up over an encrypted channel to an external audit server, if so configured.

## **4.2 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 entropy noise source.

## **4.3 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.

## **4.4 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. 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.

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 (8-127). The TOE also implements a lockout mechanism if the number of configured unsuccessful authentication attempts has been exceeded.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console, SSHv2, and HTTPS interfaces. The TOE optionally supports use of AAA server including RADIUS and TACACS+ (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE.

## **4.5 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. 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 a secure session is initially established, the TOE displays an administrator- configurable warning banner. This is used to provide any information deemed necessary by the administrator prior to logging in. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

## **4.6 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. 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.

## **4.7 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.

## **4.8 Trusted path/channels**

The TOE supports establishing trusted paths between itself and remote administrators using SSHv2 for CLI access, and TLS/HTTPS for GUI/ASDM access apart from tunneling the ASDM and/or SSH connections in IPsec VPN tunnels. The TOE supports use of TLS and/or IPsec for connections with remote syslog servers. The TOE can use IPsec to encrypt connections with remote authentication servers (e.g. RADIUS, TACACS+). 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.

## 4.9 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 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 crypto map set.

## 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 with the collaborative Protection Profile Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020 and the PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020

That information has not been reproduced here and the CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 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 CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 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 the FW and VPNGW PP-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 Network Device models was not included in the scope of the evaluation and therefore should not 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 CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

The following table list functionality excluded from the evaluation.

Excluded Functionality	Exclusion Rationale
Telnet for management purposes	Telnet passes authentication credentials in clear text and is disabled by default.
Secure Policy Manager is excluded from the evaluated configuration	Use of Security Policy Manager 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.
ASA Cluster functionality is excluded from the evaluated configuration.	Use of ASA Clustering is beyond the scope of this Common Criteria evaluation.

## 6 Documentation

The following document were available with the TOE for evaluation:

- Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series Preparative Procedures & Operational User Guide for the Common Criteria Certified configuration, Version 0.3, May 19, 2022

Only the Administrator Guide listed above, and the specific sections of the other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.”

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 be relied upon when configuring or operating the device as evaluated.

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 [9] the proprietary Detailed Test Report for Cisco Adaptive Security Appliances (ASA) 9.16 on Firepower 1000 and 2100 Series (DTR), as summarized in [8] 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 CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 including the tests associated with optional requirements. Section 3.4 of

the AAR 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 the hardware and software listed below when configured in accordance with the documentation specified in section 6. The TOE consists of the following hardware models all running the ASA 9.16 software:

- Firepower 1000 Series (1010, 1120, 1140 and 1150)
- Firepower 2100 Series (2110, 2120, 2130 and 2140)

## 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 Adaptive Security Appliances (ASA) 9.16 on Firepower 1000 and 2100 Series TOE to be Part 2 extended, and to meet the SARs contained in the CPP\_ND\_V2.2E, MOD\_CPP\_FW\_v1.4e, and MOD\_VPNGW\_v1.1.

### 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 Adaptive Security Appliances (ASA) 9.16 on Firepower 1000 and 2100 Series 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 CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 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 CPP\_ND\_V2.2E/MOD\_CPP\_FW\_v1.4e/MOD\_VPNGW\_v1.1 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 following databases:

- National Vulnerability Database (<https://web.nvd.nist.gov/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>),
- Exploit / Vulnerability Search Engine (<http://www.exploitsearch.net>),
- Tenable Network Security (<http://nessus.org/plugins/index.php?view=search>), and
- Offensive Security Exploit Database (<https://www.exploit-db.com/>).

The search was performed on June 10, 2022 and with a final update on July 15, 2022. The search was conducted with the following search terms: "ASA", "TLS", "SSH", "IPsec", "IKE", "Cisco Security Crypto", "FOM", "Xeon Processor", "Atom Processor", "Cavium Octeon III", "radius", "TACACS+", "Firepower 2100", "Firepower 1100". The evaluators found no unresolved vulnerabilities.

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

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Administrator Guide document listed in Section 6. 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 Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

## 11 Annexes

Not applicable

## 12 Security Target

The Security Target is identified as: *Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series Security Target, Version 0.5, May 18, 2022.*

## 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
- [5] collaborative Protection Profile Module for Stateful Traffic Filter Firewalls, version v1.4 + Errata 20200625, 25 June 2020
- [6] PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, 18 June 2020.



- [7] Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series Security Target, Version 0.5, May 18, 2022 (ST).
- [8] Assurance Activity Report for Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series, Version 0.2, July 15, 2022 (AAR).
- [9] Detailed Test Report for Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series, Version 0.2, July 15, 2022 (DTR).
- [10] Evaluation Technical Report for Cisco Adaptive Security Appliance (ASA) 9.16 on Firepower 1000 and 2100 Series, Version 0.2, July 15, 2022 (ETR)