National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

™

Validation Report

Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances

Report Number:	**CCEVS-VR-11090-20201**
Dated:	**January 4, 2021**
Version:	**0.2**

ACKNOWLEDGEMENTS

Table of Contents

1   Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances 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 December 2020. 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 EAL 1.

The Target of Evaluation (TOE) is the Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances.

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 ASA running on Firepower 4100 and 9300 Security Appliances Security Target, Version 1.2, December 30, 2020 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) for Evaluation Assurance Level (EAL) 1 through 4 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 ASA 9.12 running on Firepower 4100 and 9300 Security Appliances
Protection Profile	(Specific models identified in Section 3.1)
	PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020 • The PP-Configuration includes the following components: • collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (CPP_ND_V2.1) • PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 019-09-17 (CFG_NDCPP_VPNGW_V1.0) • PP-Module for Stateful Traffic Filter Firewalls, Version 1.1, 23 October 2019 (MOD_CPP_FW_1.3)
ST	Cisco ASA running on Firepower 4100 and 9300 Security Appliances Security Target, Version 1.2, December 30, 2020
Evaluation Technical Report	Evaluation Technical Report Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances, Version 0.3, December 30, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.

Item	Identifier
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc.
CCEVS Validators	Marybeth Panock, Kenneth Stutterheim

3　Architectural Information

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

The Target of Evaluation (TOE) is the Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances. The TOE is comprised of both software and hardware. The TOE hardware models include FP 4110, 4115, 4120, 4125, 4140, 4145 and 4150 and 9300. The software is comprised of the Adaptive Security Appliance software image Release 9.12, with ASDM, running on the security module and FXOS 2.6 running on Supervisor blade.

3.1　TOE Evaluated Platforms

The evaluated configuration consists of the following models:

TOE Configuration	Hardware Configurations	Software Version
FP 4110 **FP 4115** **FP 4120** **FP 4125** **FP 4140** **FP 4145** **FP 4150**	The Firepower 4100 chassis contains the following components: • Network module 1 with eight fixed SFP+ ports (1G and 10G connectivity), the management port, RJ-45 console port, Type A USB port, PID and S/N card, locator indicator, and power switch • Two network modules slots (network module 2 and network module 3) • Two (1+1) redundant power supply module slots • Six fan module slots • Two SSD bays	FXOS release 2.6 and ASA release 9.12
FP 9300	The Firepower 9300 chassis contains the following components: • Firepower 9300 Supervisor— Chassis supervisor module	FXOS release 2.6 and ASA release 9.12

	◦ Management port	
	◦ RJ-45 console port	
	◦ Type A USB port	
	◦ Eight ports for 1 or 10 Gigabit Ethernet SFPs (fiber and copper)	
	• Firepower 9300 Security Module—Up to three security modules	
	◦ 800 GB of solid state storage per security blade (2 x 800 GB solid state drives running RAID1)	
	• Firepower Network Module— Two single-wide network modules or one double-wide network module	
	• Two power supply modules (AC or DC)	
	• Four fan modules	

3.2 TOE Architecture

The TOE consists of hardware and software that provide connectivity and security services onto a single, secure device.

For firewall services, the ASA 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 the 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 VPN or remote access VPN. Other uses refer to the use of IPsec connections to tunnel traffic that originates from or terminates at the TOE itself, such as for transmissions from the TOE to remote audit/syslog servers, or AAA servers, or for an additional layer of security for remote administration connections to the TOE, such as SSH or TLS connections tunneled in IPsec.

The TOE can operate in a number of modes: as a transparent firewall with two interfaces connected to the same subnet when deployed in single-context in transparent mode; or with one or more contexts connected to two or many IP subnets when configured in routed mode.

The ASDM that allows the TOE to be managed from a graphical user interface and is an optional part of the IT environment.

3.3 Physical Boundaries

The physical boundary of the TOE is the hardware appliance. The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 1: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with SSH client installed that is used by the TOE administrator to support TOE administration through SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	The Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
ASDM Management Platform	Yes	The ASDM operates from any of the following operating systems: • Microsoft Windows 7, 8, 10, Server 2008, Server 2012, and Server 2012 R2 • Apple OS X 10.4 and later Note that that ASDM software is installed on the TOE and the management platform is used to connect to the TOE and run the ASDM. The only software installed on the management platform is a Cisco ASDM Launcher.

Component	Required	Usage/Purpose Description for TOE performance
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Connections to remote audit servers must be tunneled in IPsec or TLS.
RADIUS AAA Server	No	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators. Connections to remote AAA servers must be tunneled in IPsec.
Certification Authority	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Remote Tunnel Endpoint	Yes	This includes any peer with which the TOE participates in tunneled communications. Remote tunnel endpoints may be any device or software client that supports IPsec tunneling. Both VPN clients and VPN gateways can be considered to be remote tunnel endpoints.
NTP V3 Server	No	The TOE supports communications with an NTP V3 server. Connections to remote NTP servers can be tunneled in IPsec.

4   Security Policy

This section summaries the security functionality of the TOE:

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

4.1   Security audit

The TOE provides 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 or a configurable audit trail threshold to track

the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

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 an entropy noise source.

4.3   Full Residual 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 for ASA, and 8-80 for FXOS). The TOE also implements a lockout mechanism if the pre-configured threshold of unsuccessful attempts has been exceeded.

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. The TOE optionally supports use of any AAA server (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 an administrative session is initially established, the TOE displays an administrator-configurable warning banner. After a configurable period of inactivity, administrative sessions will be terminated, requiring administrators to re-authenticate.

4.6 Packet 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. 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. 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.

4.7 Protection of the TSF

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

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

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update

the TOE's clock manually, or can configure the TOE to use NTP V3 to synchronize the TOE's clock with an external time source. As well, the TOE performs testing to verify correct operation of the appliance itself and that of the cryptographic module. Whenever any system failures occur within the TOE the TOE will cease operation.

4.8 TOE access

When an administrative session is initially established, the TOE displays an administrator-configurable warning banner. 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 can disconnect sessions based upon idel times 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, and TLS/HTTPS for GUI/ASDM access. 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). 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.

5   Assumptions

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

- PP-Configuration for Network Devices, Stateful Traffic Filter Firewalls, and Virtual Private Network (VPN) Gateways, Version 1.0, 6 March 2020
    - o   The PP-Configuration includes the following components:
        - collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018 (CPP_ND_V2.1)
        - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17 (CFG_NDCPP_VPNGW_V1.0)
        - PP-Module for Stateful Traffic Filter Firewalls, Version 1.1, 23 October 2019 (MOD_CPP_FW_1.3)

That information has not been reproduced here and the CPP_ND_V2.1 / CFG_NDCPP_VPNGW_V1.0 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_V2.1 / CFG_NDCPP_VPNGW_V1.0 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 that may be provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

6   Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that could benefit from additional clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- 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.

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the relevant protection profiles.

- 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 scope of this evaluation was limited to the functionality and assurances covered in the CPP_ND_V2.1 / CFG_NDCPP_VPNGW_V1.0 and MOD_CPP_FW_1.3 and applicable Technical Decisions 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.

7   Documentation

The following documents were available with the TOE for evaluation:

- Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, Version 0.2, October 16, 2020

- Cisco FXOS 2.6 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, Version 0.2, October 16, 2020

The documentation listed above is the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. Any additional customer documentation provided with the product, or that may be available online, was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the product platforms as evaluated. Consumers are encouraged to download

the configuration documentation from the NIAP website to ensure that the TOE platforms are configured as evaluated.

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 ASA 9.12 running on Firepower 4100 and 9300 Security Appliances, Version 0.2, December 30, 2020 (DTR).

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 a Common Criteria Certification document and ran the tests specified in the CPP_ND_V2.1/CFG_NDCPP_VPNGW_V1.0 including the tests associated with optional requirements. The testing was performed at the Gossamer Security Solutions Common Criteria Testing Laboratory located in Catonsville, Maryland.

9   Evaluated Configuration

The evaluated Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances hardware and software is as follows:

- TOE Hardware
    - ASA Firepower 4100 Series (4110, 4115, 4120, 4125, 4140, 4145 and 4150)
    - ASA Firepower 9300 (including chassis, supervisor blade, security module)
- TOE Software
    - FXOS 2.6, ASA 9.12
- Test Configuration
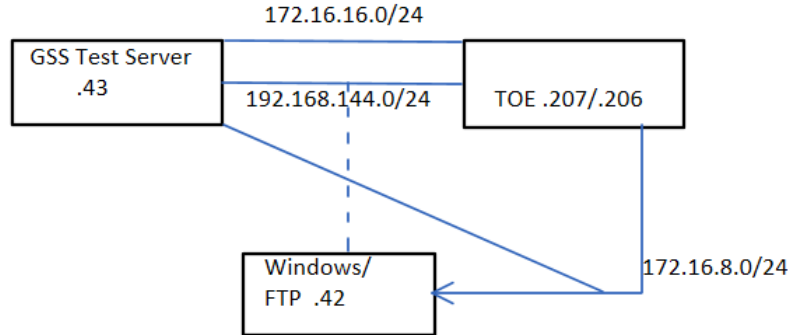
The evaluator used the following supporting software for testing:
- Ubuntu version 14.10, 64-bit
- OpenSSL version 1.0.2g
- tcpdump
- stunnel4 version 5.3
- rsyslogd version 8.16.0
- Putty version 6.2
- SecureCRT version 5.1.2
- Big Packet Putty version 6.2
- Wireshark version 1.10.0
- Nmap version 6.25

To use the product in the evaluated configuration, the product must be configured as specified in the following documents.

- Cisco Adaptive Security Appliance (ASA) 9.12 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, Version 0.2, October 16, 2020
- Cisco FXOS 2.6 on Firepower 4100 and 9300 Preparative Procedures & Operational User Guide for the Common Criteria Certified Configuration, Version 0.2, October 16, 2020

10 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.

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.

10.1 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 ASA 9.12 running on Firepower 4100 and 9300 Security Appliances products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validators 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.

10.2 Evaluation of the Development (ADV)

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_V2.1 / CFG_NDCPP_VPNGW_V1.0 related to the examination of the information contained in the TSS.

The validators 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.

10.3 Evaluation of the Guidance Documents (AGD)

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 validators 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.

10.4 Evaluation of the Life Cycle Support Activities (ALC)

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.

10.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team ran the set of tests specified by the assurance activities in the CPP_ND_V2.1 / CFG_NDCPP_VPNGW_V1.0 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.

10.6 Vulnerability Assessment Activity (VAN)

The evaluation team performed a public search for vulnerabilities on December 23, 2020 at the following sites and did not discover any public issues with the TOE. The evaluator searched the following sources for vulnerabilities:

- 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 Engin (http://www.exploitsearch.net),
- SecurITeam Exploit Search (http://www.securiteam.com),
- Tenable Network Security (http://nessus.org/plugins/index.php?view=search),
- Offensive Security Exploit Database (https://www.exploit-db.com/)

The terms used for the search were as follows: "Cisco", "FXOS", "ASA", "Firepower 4100", "Firepower 9300", "radius", "TACACS+", "ssh", "tls", "ike", "ipsec", "Firewall", "VPN Gateway", "router", "TCP", "ldap".

In addition, the evaluation team performed testing against the TOE with fuzzed, mutated, invalid and undefined packets and noticed no ill effects exhibited by the TOE as a result.

The validators 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.

10.7 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.

11 **Validator Comments/Recommendations**

None

12 **Annexes**

Not applicable

13 **Security Target**

Cisco ASA running on Firepower 4100 and 9300 Security Appliances Security Target, Version 1.2, December 30, 2020.

14 **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.

15 **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 2.1, 24 September 2018 (CPP_ND_V2.1),

[5]   PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 17 September 2019 (CFG_NDCPP_VPNGW_V1.0)

[6]   Cisco ASA running on Firepower 4100 and 9300 Security Appliances Security Target, Version 1.2, December 30, 2020 (ST)

[7]   Assurance Activity Report for Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances, Version 0.3, December 30, 2020 (AAR)

[8]   Detailed Report for Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances, Version 0.2, December 30, 2020 (DTR)

[9]   Evaluation Technical Report for Cisco ASA 9.12 running on Firepower 4100 and 9300 Security Appliances, ETR, Version 0.3, December 30, 2020 (ETR)