National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Stealthwatch Enterprise 7.1

Report Number: CCEVS-VR-11059-2020
Dated: 07/21/2020
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Paul Bicknell, Senior Validator
Jenn Dotson, ECR Team
Linda Morrison, ECR Team
Lisa Mitchell, Lead Validator

Common Criteria Testing Laboratory

Cody Cummins
Katie Sykes
Gossamer Security Solutions, Inc.
Catonsville, MD

Table of Contents

Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Stealthwatch Enterprise 7.1 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 Catonsville, MD, United States of America, and was completed in July 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 the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1, 24 September 2018.

The Target of Evaluation (TOE) is the Cisco Stealthwatch Enterprise 7.1.

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 (CCEVS) 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 Stealthwatch Enterprise 7.1 Security Target, Version 1.1, July 17, 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) 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 Stealthwatch Enterprise 7.1 (Specific models identified in Section 8)
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018
ST	Cisco Stealthwatch Enterprise 7.1 Security Target, Version 1.1, July 17, 2020
Evaluation Technical Report	Evaluation Technical Report for Cisco Stealthwatch Enterprise 7.1, version 0.3, 07/17/2020
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.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Catonsville, MD
CCEVS Validators	Paul Bicknell Jenn Dotson Linda Morrison Lisa Mitchell

3 Architectural Information

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

The Cisco Stealthwatch Enterprise TOE is a centrally managed system of distributed components for collection, storage, analysis, of network telemetry data. The evaluated configurations of the TOE consist of one Stealthwatch Management Console (SMC), one or more Flow Collectors (FC), one or more Flow Sensors (FS), and one or more UDP Directors (UDPD). Each of the TOE components is available as a stand-alone physical appliance, or as a virtual appliance. The physical and virtual appliances provide equivalent functionality and a mixture of physical and virtual appliances can be deployed together.

Cisco Stealthwatch Enterprise provides visibility and security analytics (threat detection, and threat response) using on network traffic telemetry data. Stealthwatch Enterprise can generate telemetry data directly (by directly monitoring traffic flows), or can collect telemetry data generated by devices in an existing network infrastructure.

3.1 TOE Evaluated Configuration

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

3.2 TOE Architecture

The TOE is a system comprised of four types of servers, each of which is comprised of both software and hardware. The software is a proprietary build of Linux with Cisco Stealthwatch applications; the hardware is Cisco UCS server platforms, which are used for the physical appliances as well as for virtual appliances. The software is comprised of the Stealthwatch software image Release 7.1.

The Cisco Stealthwatch Enterprise components that comprise the TOE have common hardware characteristics. Any hardware differences, e.g. the amount of RAM or drive space, of the number of network interfaces, affect only non-TSF relevant functionality such as throughput and amount of storage, and therefore support security equivalency of the TOE component models.

This TOE is considered a ‘distributed’ TOE as defined in NDcPP in that this TOE requires multiple distinct TOE components to operate as a logical whole in order to fulfil the requirements of NDcPP, and those TOE components are separated (distributed) across a network. This TOE includes one management component (SMC), and three types of managed network devices (FC, FS, and UDPD).

The Stealthwatch Management Console (SMC) provides the administrative interface to manage all TOE components. The SMC aggregates, organizes, and presents analysis from up to 25 Flow Collectors, the Cisco Identity Services Engine, and other sources.

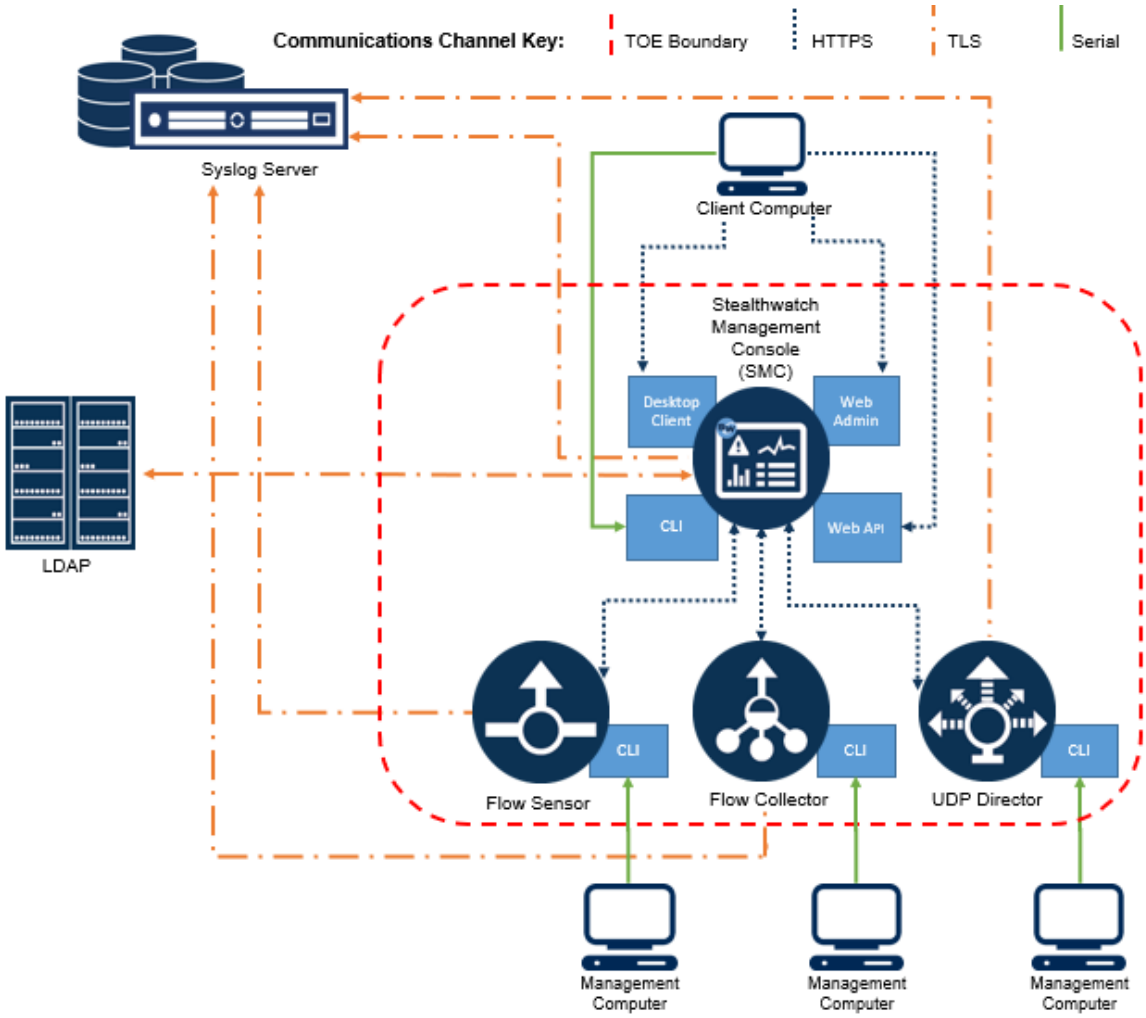
The Stealthwatch Flow Collector (FC) receives telemetry data from Stealthwatch Flow Sensors and other sources such as routers, switches, firewalls, and endpoint agents. The FC stores collected data in its internal database, analyses the data, sends event notifications to SMC, and supports further forensics and long-term data analysis via customized reporting

provided by the SMC. Multiple Flow Collectors may be managed by a single SMC and are available as hardware appliances or as virtual machines.

The Flow Sensor (FS) produces telemetry for segments of the switching and routing infrastructure that cannot generate NetFlow natively. The Flow Sensors connect directly to a mirroring port or network tap to monitor network traffic and generate telemetry data. Multiple Flow Sensors can be managed by a single SMC and are available as hardware appliances or as virtual appliances to monitor virtual machine environments.

The UDP Director (UDPD) simplifies the collection and distribution of network and security data across the enterprise. It helps reduce the processing power on network routers and switches by receiving essential network and security information from multiple locations and then forwarding it to a single data stream to one or more destinations. Multiple UDP Directors can be managed by a single SMC and are available as hardware appliances or as virtual appliances to monitor virtual machine environments.

The TOE consists of one or more physical devices and includes the Cisco Stealthwatch software. The figure below shows each of the four TOE components in the operational environment. The diagram shows one of each appliance (SMC, FC, FS, and UDPD), where each appliance can be either physical or virtual. The diagram shows only a single icon for the FC though the FC physical appliance is available in two forms: as a single appliance (FC4210) with the engine and database installed to the same appliance; or as a pair of appliances with the FC Engine on one appliance (FC5200E) and the FC Database on the other appliance (FC5200D). Regardless of the form-factor, each FC model provides the same TOE security functionality.



This figure shows the protocols and connections (TLS, HTTPS, and the serial connections) that are relevant to requirements within NDcPP. The TOE components also use other protocols (e.g. domain name service (DNS), NetFlow and sFlow) that are not relevant to NDcPP requirements as that traffic does not contain TSF data. Each appliance contains a DNS client for fully qualified domain name (FQDN) resolution (e.g. for lightweight directory access protocol (LDAP) servers, certification authorities (CAs), uniform resource locator (URL) distribution points, and online certificate status protocol (OCSP) responders). The FC receives NetFlow or sFlow traffic (depending on whether the FC was installed in sFlow or NetFlow mode) from UDPD and FS. The FS monitors network traffic (via its promiscuous (passive) interface) and generates sFlow or NetFlow data to transmit to an FC. The UDPD receives sFlow or NetFlow traffic from monitored devices and forwards that traffic to an FC.

3.3 Physical Boundaries

The TOE is a hardware and software solution composed of four major components: SMC, FC, FS, and UDPD. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE and

includes the Cisco Stealthwatch Compliance Guide and additional guidance documents referenced therein, all of which are downloadable from the http://cisco.com web site. The TOE is comprised of the physical specifications as described in Section 8 below.

The ST identifies the following hardware, software and firmware in the operating environment of the TOE:

- Management workstation with transport layer protocol (TLS) client (browser) – required
- Management workstation with console connection – required
- Certification Authority – required
- LDAP Server – optional (the TOE also provides local authentication)
- Syslog Server - required

4 Security Policy

This section summaries 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

4.1 Security audit

The Cisco Stealthwatch Enterprise provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Stealthwatch Enterprise generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, configures secure transmission of audit records to a remote audit server, and manages audit data storage. The TOE provides the administrator with a local circular audit trail. Audit messages are stored locally and transmitted over an encrypted channel to an external audit server.

4.2 Communication

The TOE allows authorized administrators to control which Stealthwatch appliance (FC, FS, and UDPD) is managed by the SMC. This is performed through a registration process over TLS. The administrator can also de-register an appliance if he or she wishes to no longer manage it through the SMC. For this TOE the process of registration/joining a new managed appliance (FC, FS, UDPD) to the SMC is manually initiated by the administrator installing each appliance. The initial TLS connection is authenticated to the SMC using the

SMC administrator's username/password, at which point the appliances exchange their X.509 certificates, and from that point forward all TLS communications among appliances are authenticated using X.509 certificates.

4.3 Cryptographic support

The TOE provides cryptography in support of other Cisco Stealthwatch security functionality. This cryptography has been validated by the NIST CAVP.

The TOE provides cryptography in support for TLS, which is used for remote administrative management, and secure communication among TOE components, and connects from the TOE to LDAP and syslog servers. The cryptographic services provided by the TOE are described in the table below.

Cryptographic Method	Use within the TOE
AES	Used to encrypt TLS session traffic.
ECDH	Used to provide key exchange in TLS.
RSA Signature Services	X.509 certificate signing and verification. Data signing and verification in TLS.
HMAC	Used for keyed hash, integrity services in TLS session establishment.
DRBG	Used for random number generation Used in TLS session establishment.
SHA	Used to provide TLS traffic integrity verification
Transport Layer Security (TLS)	Used in TLS session establishment.

During initial installation each TOE component generates its own unique self-signed X.509v3 certificate, and during initial configuration all those certificates are replaced with new CA-signed identity certificates which are then used for all TLS connections including mutual authentication of TLS connections among TOE components. Each TOE component generates its own unique keypair and its own certificate signing requests (CSR), and imports TLS certificates that have been signed by an external CA server.

4.4 Identification and authentication

TOE components perform two types of authentication: password-based authentication of administrators for remote administration TOE; and certificate-based authentication of devices. Device-level authentication allows TOE components to establish secure channels with other TOE components, and with external servers (LDAP and syslog).

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console, and the GUI (accessible via HTTPS/TLS). For authentication to the GUI, the TOE optionally supports use of an authentication, authorization, and accounting (AAA) server (using LDAP over TLS), which would be outside the TOE boundary.

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.

After a configurable number of incorrect login attempts at administrative interfaces where authentication is processed locally (i.e. where LDAP is not used), the TOE will lock the offending account until an Administrator defined time period has elapsed.

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 HTTPS/TLS 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 updates to the TOE.

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 set amount of time of inactivity, the administrator will be locked out of the administrator interface.

4.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of plaintext cryptographic keys and passwords.

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.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. The TOE performs self-testing to verify correct operation of its cryptographic module. The TOE components are not general-purpose operating systems; root access is not permitted, external software applications cannot be installed, and access to memory space is restricted to TOE functions.

The TOE is distributed, including multiple appliances that communicate with each other over a network. These internal TOE communications between TOE components are protected within TLS, and authenticated using X.509 certificates.

4.7 TOE access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface and the WebUI prior to allowing any administrative access to the TOE.

4.8 Trusted path/channels

The TOE establishes a trusted path with syslog servers using TLS, and with LDAP servers using TLS. Remote administration of the TOE uses TLS/HTTPS. All communications between TOE components are protected within TLS; the initial joining of TOE components is authenticated using a username and password that's manually entered during the joining process, and subsequent communications between TOE components are automatically authenticated using X.509 certificates.

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 2.1, 24 September 2018

That information has not been reproduced here and the NDcPP21 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 NDcPP21 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 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.
- 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 NDcPP21 and applicable Technical Decisions. Any

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

6 Documentation

The following documents were available with the TOE for evaluation:

- Cisco Stealthwatch Compliance Guide 7.1, Version 1.0, July 2, 2020

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP21) for Cisco Stealthwatch Enterprise 7.1, Version 0.3, 07/17/2020 (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 a Common Criteria Certification document and ran the tests specified in the NDcPP21 including the tests associated with optional requirements.

8 Evaluated Configuration

The evaluated configuration consists of the following physical and virtual devices all running Cisco Stealthwatch software release 7.1.

Appliance	Part Number	Server platform	Entropy Source
Stealthwatch appliances on UCS C-Series M5 servers			
Stealthwatch Management Console	ST-SMC2210-K9 L-ST-SMC-VE-K9	UCSC-C220-M5SX	Intel® Skylake Scalable Processor
Stealthwatch UDP Director	ST-UDP2210-K9 L-ST-UDP-VE-K9		
Stealthwatch Flow Sensor	ST-FS1210-K9 ST-FS3210-K9 ST-FS4210-K9 L-ST-FS-VE-K9		
Stealthwatch Flow Collector	ST-FC4210-K9 L-ST-FC-VE-K9		
Stealthwatch Flow Collector Engine	ST-FC5210E		
Stealthwatch Flow Collector Database	ST-FC5210D	UCSC-C240-M5SX	
Stealthwatch appliances on UCS C-Series M4 servers			
Stealthwatch Management Console	ST-SMC2200-K9 L-ST-SMC-VE-K9	UCSC-C220-M4S	Intel® Xeon® E5-26XX

Stealthwatch UDP Director	ST-UDP2200-K9 L-ST-UDP-VE-K9		
Stealthwatch Flow Sensor	ST-FS1200-K9 ST-FS2200-K9 ST-FS3200-K9 ST-FS4200-K9 L-ST-FS-VE-K9		
Stealthwatch Flow Collector	ST-FC4200-K9, or L-ST-FC-VE-K9		
Stealthwatch Flow Collector Engine	ST-FC5200E		
Stealthwatch Flow Collector Database	ST-FC5200D	UCSC-C240-M4S2	

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 Stealthwatch Enterprise 7.1 TOE to be Part 2 extended, and to meet the security assurance requirements (SARs) contained in the NDcPP21.

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 Stealthwatch Enterprise 7.1 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 NDcPP21 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 NDcPP21 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 evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- 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)
- 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 search was performed on 06/22/2020 with the following search terms: “TCP", "router", "switch", "TLS", "Cisco", "Stealthwatch".

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. Cisco Stealthwatch Compliance Guide, Version 1.0, July 2, 2020. This includes ensuring that network time protocol (NTP) communication, which is enabled by default, is properly disabled. In addition, the Cisco Stealthwatch Compliance Guide contains compliance guidance for the Department of Defense Information Network (DoDIN) approved products list (APL) as well as the CC PCL; the Compliance Configuration Overview section indicates the sections of the document that apply to each. Care must be taken to follow the guidance for those sections marked as required for CC in order to place the TOE in the evaluated configuration.

The validation team notes that each TOE component listens on the default TLS/HTTPS port; however, only the SMC supports remote authentication. Remote login is disabled on the other components.

The validation team notes that the TOE supports reference identifiers in either the Common Name (CN) and the Subject Alternative Name (SAN) extension in X.509 certificates; however, for inter-component communications, the SAN extension is required.

11 Annexes

Not applicable

12 Security Target

The Security Target is identified as: *Cisco Stealthwatch Enterprise 7.1 Security Target, Version 1.1, July 17, 2020*.

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 2.1, 24 September 2018.

[5] Cisco Stealthwatch Enterprise 7.1 Security Target, Version 1.1, July 17, 2020 (ST).

[6] Assurance Activity Report (NDcPP21) for Cisco Stealthwatch Enterprise 7.1, Version 0.3, 07/17/2020 (AAR).

[7] Detailed Test Report (NDcPP21) for Cisco Stealthwatch Enterprise 7.1, Version 1.2, 06/29/2020 (DTR).

[8] Evaluation Technical Report for Cisco Stealthwatch Enterprise 7.1, Version 0.3, 07/17/2020 (ETR)