National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Identity Services Engine (ISE) V2.2 on the 3415, 3515, 3495 and 3595 Appliances

Report Number: CCEVS-VR-10858-2018

Dated: 04/13/2018

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

Patrick Mallett, PhD.

MITRE Corporation

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Micciche

Kevin Zhang

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the validator comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Identity Services Engine (ISE) V2.2 Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in April 2018. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the collaborative Protection Profile for Network Devices Version 1.0 (NDcPPv1.0) and Extended Package for Authentication Server Version 1.0 (AUTHSRVEPv1.0).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP 1.0 and AUTHSRVEP 1.0. 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 provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, 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.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

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 Product Compliance 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 results of the evaluation.
- The Protection Profile(s) 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 Identity Services Engine (ISE) V2.2
Protection Profile	NDcPP 1.0, AUTHSRVEP 1.0
Security Target	Cisco Identity Services Engine (ISE) V2.2 Security Target, Version 1.0
Evaluation Technical Report	Cisco Identity Services Engine (ISE) V2.2 ETR, Version 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Patrick Mallett, PhD., Kenneth Stutterheim

3 Architectural Information

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

This section provides an overview of the Cisco Identity Services Engine (ISE) v2.2, Patch2 Target of Evaluation (TOE) and a brief description of the capabilities of the ISE product. ISE is a consolidated policy-based access control system that combines authentication, authorization, accounting (AAA), posture, profiler, and guest management in one appliance. ISE v2.2 software runs on the Cisco Application Deployment Engine (ADE) Release 3.0 operating system (ADE-OS).

The TOE also includes an instance of the Embedded Services Router 5921 [ESR], running IOS 15.5(3)M5. The ESR is a software-only solution for routing capabilities. The ESR provides IPsec session capabilities for ISE v2.2 to secure the channel between the TOE and NAS. The IOS image runs as a process on the bundle included in the ADE-OS.

3.1 TOE Evaluated Platforms

Cisco ISE software runs on a dedicated Cisco ISE 3400/3500 Series appliance. All models include the same security functionality. The hardware models include ISE appliances 3415, 3495, 3515, and 3595.

3.2 TOE Architecture

The evaluated configuration is a single ISE instance. A typical deployment will include network devices utilizing the ISE authentication, authorization and accounting (AAA) features, remote administrator, local administrative console and a remote authentication store. Both the remote administrator and local administrator console capabilities must be supported.

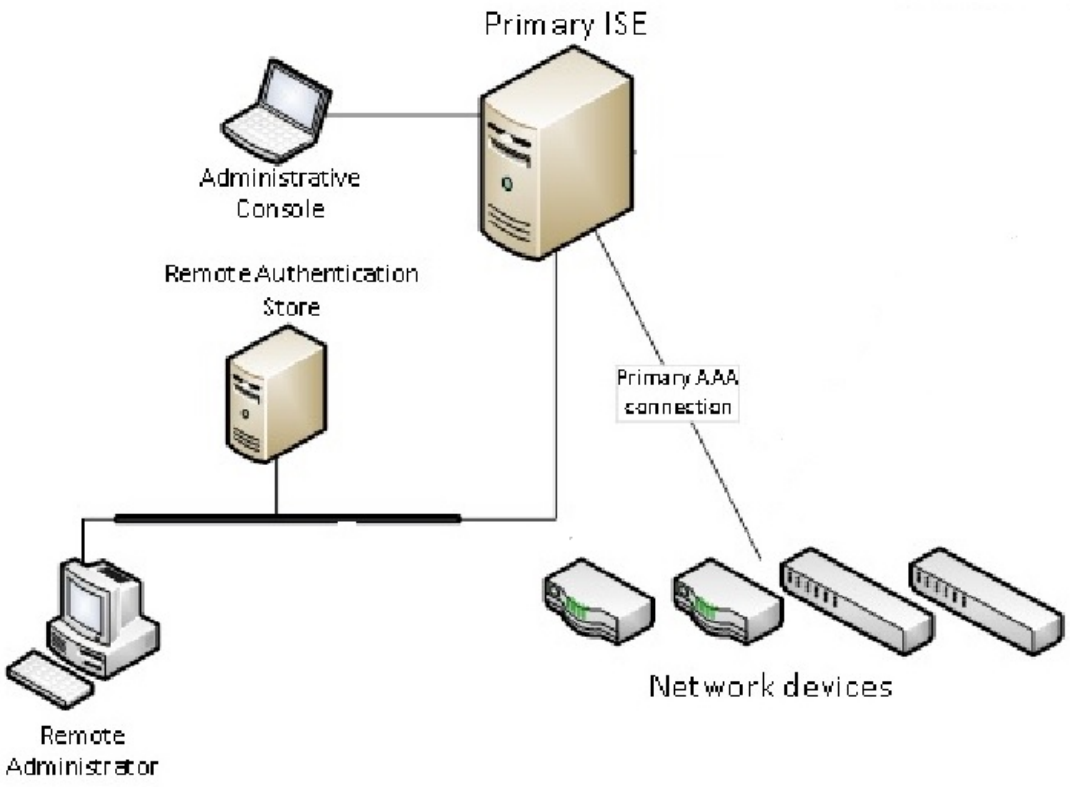


Figure 1: TOE Deployment

3.3 Physical Boundaries

The TOE is comprised of the following physical specifications as described in Table 2 below:

Hardware Model	Cisco Identity Services Engine Appliance 3415	Cisco Identity Services Engine Appliance 3495	Cisco Identity Services Engine Appliance 3515	Cisco Identity Services Engine Appliance 3595
Processor	Intel Xeon	Intel Xeon	Intel Xeon	Intel Xeon
Memory	16 GB	32 GB	16 GB	64 GB
Hard disk	1x600Gb disk	2x600Gb disk	1x600Gb disk	4x600Gb disk
RAID	Yes (Software RAID level 0	Yes (RAID 1)	Yes (Software RAID level 0 (single drive striped))	Yes (RAID 0+1)

Hardware Model	Cisco Identity Services Engine Appliance 3415	Cisco Identity Services Engine Appliance 3495	Cisco Identity Services Engine Appliance 3515	Cisco Identity Services Engine Appliance 3595
	(single drive striped))			
Expansion slots	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)	- Two PCIe slots (on a riser card)
Serial port (RJ-45 Connector)	1	1	1	1
USB 2.0 ports	2	2	0	0
USB 3.0 ports	0	0	2	2
1-GB Ethernet Management Port	1	1	1	1
Video ports	1	1	1	1

4 Security Policy

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptographic Support
3. Communications
4. Identification and Authentication
5. Security Management
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

4.1 Security Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. The events generated by the TOE include indication of the logging starting and stopping, cryptographic operations, attempts to log onto the TOE, all commands/ web-based actions executed by the Security Administrator, and other system events.

The TOE can store the generated audit data on itself and it can be configured to send syslog events to other devices, including other iterations of ISE, using a TLS protected collection method. Access to the logs is restricted only to the Security Administrator, who has no access to edit them, only to copy or delete (clear) them. Audit records are protected from unauthorized modifications and deletions.

The log record includes the category name, the message class, the message code (type of event), the message text (including a date/time stamp, subject (user) associated with the event, outcome of the event, etc.) and the severity level associated with the message. The previous audit records are overwritten when the allocated space for these records reaches the threshold.

4.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; asymmetric key generation; cryptographic key establishment using RSA-based key establishment schemes and DH key establishment; digital signature using RSA; cryptographic hashing using SHA1 (and other sizes); random bit generation using DRBG and keyed-hash message authentication using HMAC-SHA (multiple key sizes). ISE uses the Cisco

FIPS Object Module (FOM) crypto library as its cryptographic module. The TOE implements the secure protocols - SSH and TLS/HTTPS on the server side and TLS on the client side.

4.3 Communications

The TOE can validate the NAS and prevent it from being spoofed. It receives the transmitted Access-Request and identifies its origin. The TOE can validate the authenticity of the NAS by verifying the Message Authenticator that is computed in part using a shared secret known to both the NAS and the TOE as defined in RFC 3579. It then returns a valid response to the NAS upon receipt of an Access-Request. The response contains the necessary information to the recipient of that message that identifies the TOE as the valid recipient of the original Access-Request and the Access-Request that elicited the response from the TOE.

4.4 Identification and Authentication

All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. Once a user attempts to access the management functionality of the TOE, the TOE prompts the user for a user name and password for remote password-based authentication. The identification and authentication credentials are confirmed against a local user database or an optional remote authentication store (part of the IT Environment). Other authentication options include public key authentication. For remote password-based authentication to the administration application, an Active Directory identity source (remote authentication store) is required to perform the association of the credentials to an ISE Role Based Access Control role. For the SSH public key authentication method, public keys will be used for signature verification. The user information is from the local user database. It is only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

The TOE provides the capability to set password minimum length rules. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

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 session, a terminal server or a local console connection. The TOE provides the ability to perform the following actions:

- Administer the TOE locally and remotely
- Configure the access banner
- Configure the cryptographic services
- Update the TOE and verify the updates using digital signature capability prior to installing those updates

- Specify the time limits of session inactivity

All of these management functions are restricted to the Security Administrator of the TOE, the individuals who manage specific type of administrative tasks. The Security Administrators are dependent upon the admin role assigned to them, which limits the network access or tasks they can perform (a role-based access approach).

The primary management interface is the HTTPS Cisco ISE user interface. The management services include authentication, authorization, posture, guest, profiler, as well as monitoring, troubleshooting, and reporting. A Command Line Interface (CLI) is also supplied for additional administration functionality like system-level configuration in EXEC mode and other configuration tasks in configuration mode and to generate operational logs for troubleshooting. This interface can be used remotely over SSHv2.

4.6 Protection of the TSF

The TOE provides protection of TSF data (authentication data and cryptographic keys). In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. This time can be set manually. Finally, the TOE performs testing to verify correct operation. The TOE is also capable of ensuring software updates are from a reliable source. In order for updates to be installed on the TOE, an administrator must use the digital signature mechanism to confirm the integrity of the product.

4.7 TOE Access

The TOE can terminate inactive sessions after a Security Administrator configurable time-period. The TOE also allows users to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display a Security Administrator specified banner on the CLI and the web-based management interface prior to allowing any administrative access to the TOE.

4.8 Trusted Path/Channel

The TOE establishes a trusted path between the ISE and the administrative web-based UI using TLS/HTTPS, and between the ISE and the CLI using SSH. The TOE also establishes a secure connection for sending syslog data to other IT devices and other external authentication stores using TLS-protected communications.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 2: TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.NAS	It is assumed that the TOE is connected to a Network Access Server (NAS) located in the Operational Environment that transmits authentication requests to it.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 3: Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

Threat	Threat Definition
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

Threat	Threat Definition
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.
T.FALSE_ENDPOINTS	A malicious actor may falsely impersonate the TOE or the NAS in order to cause the TOE to operate in an insecure manner or to extract security-relevant data from the TOE or its Operational Environment.
T.INVALID_USERS	A malicious user may supply incorrect credential data or an otherwise invalid authentication request that is approved or ignored by the TSF such that protected resources in the Operational Environment are subject to unauthenticated access.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. 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 level of assurance for this evaluation is defined within the NDcPP 1.0 and AUTHSRVEP 1.0.
- 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.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Identity Services Engine (ISE) V2.2 Security Target, Version 1.0
- Cisco Identity Services Engine (ISE) V2.2 Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0

Any additional customer documentation delivered with the product or that is available through download was not included in the scope of the evaluation, and therefore should not be relied upon when configuring or using the products as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a hardware and software solution as follows:
Cisco Identity Services Engine (ISE) v2.2, Patch2 software on the following hardware appliances:

- Cisco ISE 3415
- Cisco ISE 3495
- Cisco ISE 3515
- Cisco ISE 3595

7.2 Excluded Functionality

In addition to any functionality not covered by Security Functional Requirements (SFRs) in the NDcPPv1.0 and AUTHSRVEPv1.0, the following functionality is excluded from the evaluation:

Table 4: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
All functional capabilities of Cisco ISE that have not been described in Section 6.1 of the Security Target for this evaluation.	These functionalities do not map to the NDcPP requirements.

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 Test Plan for the TOE, and summarized in the Common Criteria Assurance Activity Report for Cisco Identity Services Engine (ISE) V2.2 (AAR), which is publicly available.

8.1 Developer Testing

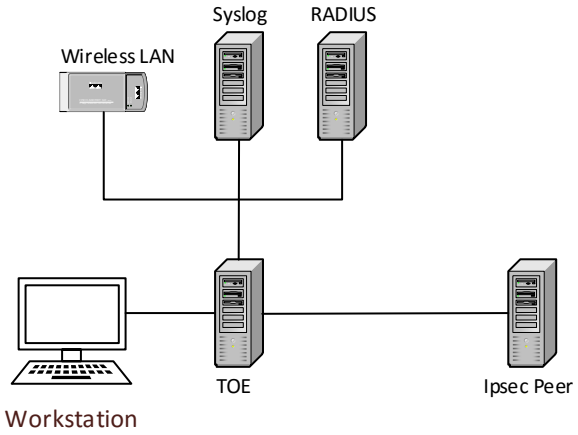
No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 1.0 and AUTHSRVEP 1.0. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

8.2.1 Test Bed

The following is a simple diagram of the test infrastructure used by the evaluators:



8.2.1.1 Configuration Information

The following provides configuration information about each test device and test tool on the test network.

8.2.1.2 Cisco ISE

- Software Version: ISE 2.2
- Username/Password: Varies per test

8.2.1.3 Peer Router

- Software Version: IOS-XE 16.3

- Username/Password: Varies per test

8.2.1.4 Test Tools

- Kiwi Syslog
- OpenSSL
- OpenRADIUS
- Cisco Wireless LAN Controller
- Wireshark
- Workstation running Windows 10 and Kali Linux Virtual Machine

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 documents: The Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). Those results are summarized in the publicly available Assurance Activity Report for this evaluation. The reader of this document can assume that 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 4 and CEM version 3.1 rev 4. The evaluation determined TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP 1.0 and AUTHSRVEP 1.0.

9.1 Evaluation of 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 TOE that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the NDcPP 1.0 and AUTHSRVEP 1.0.

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.

9.2 Evaluation of Development Documentation (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's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP 1.0 and AUTHSRVEP 1.0 related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the NDcPP 1.0 and AUTHSRVEP 1.0 related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

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.

9.5 Evaluation of 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 NDcPP 1.0 and AUTHSRVEP 1.0 and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validators reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDcPP 1.0 and AUTHSRVEP 1.0, 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 Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/

The evaluator performed the public domain vulnerability searches using the following key terms.

- Cisco Systems, Inc

- Identity Services Engine Version 2.2
- Cisco ISE
- ISE 3400
- ISE 3500

The evaluator selected these and other search key words based upon the following criteria.

- The vendor name was searched,
- The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched,
- The name of the hardware devices within the TOE,
- The secure protocols supported by the TOE,
- The type of TOE device.

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 addressed the vulnerability analysis Assurance Activities in the NDcPP 1.0 and AUTHSRVEP 1.0, 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 test activities 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 performed the Assurance Activities in the NDcPP 1.0 and AUTHSRVEP 1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

Administrators are cautioned to understand the evaluated configuration of the product. The product offers functionality that was not evaluated, and no claims can be made regarding the effectiveness of the additional functionality as noted above in section 7.2.

Also, the TSS of the Security Target explicitly states that only main mode IKEv1 Phase 1 exchanges are supported and aggressive mode exchanges are rejected. This must be configured when setting the device into the evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

Cisco Identity Services Engine (ISE) V2.2 on the 3415, 3515, 3495 and 3595 Appliances Security Target, Version 1.0

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Cisco Identity Services Engine (ISE) V2.2 on the 3415, 3515, 3495 and 3595 Appliances Security Target, Version 1.0, April 13, 2018
6. Common Criteria NDCPP Assurance Activity Report for Cisco Identity Services Engine (ISE) V2.2 Version 1.3, 04.13.2018 (AAR)
7. Cisco Identity Services Engine (ISE) V2.2 Evaluation Technical Report, Version 1.1 April 13, 2018 (ETR) < evaluation sensitive document>
8. Cisco Identity Services Engine (ISE) V2.2 Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0, April 2018
9. Test Plan for a Cisco ISE 2.2 NDcPP 1.0 with AUTHSRV 1.0 <evaluation sensitive document>