National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco Identity Services Engine (ISE)

Report Number: CCEVS-VR-VID10521-2014
Version 1.0
January 30, 2014

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

Jandria Alexander, Senior Validator
The Aerospace Corporation

Kenneth Stutterheim, Lead Validator
The Aerospace Corporation

Common Criteria Testing Laboratory

Chris Gugel, CC Technical Director
Justin Fisher
Josh Jones
Jeff Barbi
Kevin Le
Jeremy Sestok
Andrea Wright

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of Cisco Identity Services Engine (ISE), 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in January 2014. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP).

The Target of Evaluation (TOE) is the Cisco Identity Services Engine (ISE), with software version 1.2, with patch 5 (1.2.0.899-5). The Cisco ISE TOE is an identity and access control platform that enables organizations to enforce compliance and security within the network infrastructure.

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 NDPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDPP Assurance Activities. 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 Identity Services Engine (ISE) Security Target, Version 1.0, January 2014 and analysis performed by the Validation Team.

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 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 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 Identity Services Engine (ISE) v1.2, with patch 5 (1.2.0.899-5) *Refer to Table 2 for Models and Specifications
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional IPSec requirements)
Security Target	Cisco Identity Services Engine (ISE) Security Target, Version 1.0, January 2014
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Cisco Identity Services Engine (ISE)" Evaluation Technical Report v3.0 dated January 21 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Jandria Alexander, The Aerospace Corporation Kenneth Stutterheim, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

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

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNDETECTED_ACTIONS** — Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.PROTECTED_COMMUNICATIONS** — The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- **O.VERIFIABLE_UPDATES —** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- **O.SYSTEM_MONITORING** — The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- **O.DISPLAY_BANNER** — The TOE will display an advisory warning regarding use of the TOE.
- **O.TOE_ADMINISTRATION** — The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.RESIDUAL_INFORMATION_CLEARING** — The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.SESSION_LOCK —** The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.TSF_SELF_TEST —** The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly**.**

3.4 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 Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional IPSec requirements) to which this evaluation claimed exact compliance.
- 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 TOE includes all the code that enforces the policies identified (see Section 5).

The evaluated configuration of the TOE includes the Cisco Identity Services Engine (ISE) v1.2, with patch 5 (1.2.0.899-5) product that is comprised of one or more of the product models.

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

4 Architectural Information

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

4.1 TOE Introduction

The Target of Evaluation (TOE) is the Cisco Identity Services Engine (ISE). The ISE architecture supports both stand-alone and distributed deployments. In a distributed configuration, one machine assumes the primary role and another "backup" machine assumes the secondary role. The TOE consists of one or more models as specified in Section 4.2 below and includes the software version 1.2, with patch 5 (1.2.0.899-5).

The administrator can deploy ISE nodes with one or more of the Administration, Monitoring, and Policy Service personas, each one performing a different vital part in the overall network policy management topology. Installing ISE with an Administration persona allows the administrator to configure and manage the network from a centralized portal. The administrator can also choose to deploy the ISE platform as an Inline Posture node to perform policy enforcement

4.2 Physical Boundaries

The Cisco ISE software runs on the Cisco Application Deployment Engine (ADE) Release 2.0 operating system (ADE-OS). The Cisco ADE-OS and Cisco ISE software run on a Cisco ISE 3400 Series appliance or on a dedicated hardware platform with a VMWare hypervisor; the hardware specifications must meet the requirements defined in the table below. All models include the same security functionality.

Table 2 – Hardware Models and Specifications

Hardware Model	**Cisco Identity Services Engine Appliance 3415 (Small)**	**Cisco Identity Services Engine Appliance 3495 (Large)**	**Cisco Identity Services Engine Virtual Machine (on dedicated hardware[1]) Required minimum system specifications[2]**
Processor	Cisco UCS C220M3, Single Intel Xeon E5-2609 4 core processor	Cisco UCS C220M3, Dual Intel Xeon E5-2609 4 core processor (8 cores total)	Single Quad-Core; 2.13 GHz or faster
Memory	16 GB	32 GB	4 GB
Hard disk	1x600Gb disk	2x600Gb disk	100 to 600 GB of disk storage (size depends on deployment and tasks) with SCSI controller
RAID	Yes (Software RAID level 0 (single drive striped))	Yes (RAID 1)	N/A
Expansion slots	- Two PCIe slots (on a riser card) ■One full-height profile, half-length slot	- Two PCIe slots (on a riser card) ■One full-height profile, half-length slot with x24	N/A

Hardware Model	Cisco Identity Services Engine Appliance 3415 (Small)	Cisco Identity Services Engine Appliance 3495 (Large)	Cisco Identity Services Engine Virtual Machine (on dedicated hardware[1]) Required minimum system specifications[2]
	with x24 connector and x16 lane ■One half-height profile, half-length slot with x16 connector and x8 lane	connector and x16 lane ■One half-height profile, half-length slot with x16 connector and x8 lane	
NIC Ports	■ One 1-GB Ethernet port (GigE0) for TOE management and network device governance ■ Three 1-GB Ethernet ports (GigE1, GigE2, GigE3) for network device governance	■ One 1-GB Ethernet port (GigE0) for TOE management and network device governance ■ Three 1-GB Ethernet ports (GigE1, GigE2, GigE3) for network device governance	1-GB Ethernet port required for TOE management and network device governance (two or more NICs are recommended)
Serial/VGA ports	2	2	N/A
USB 2.0 ports	2	2	N/A
Video ports	1	1	N/A
External SCSI ports	None	None	N/A
Hypervisor	None	None	• VMware ESX 4.x • VMware ESXi 4.x; or • VMware ESXi5.x

1. ISE Virtual Machine's hardware must be dedicated. Likewise, the virtual resources will be dedicated to a single virtual machine running the ISE software.
2. It is recommended that the system specification be comparable with the 3415 or 3495 models in a production environment. This table lists the minimum system specifications for the ISE Virtual Machine to operate as validated by this evaluation.

The TOE resides on a network and supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 – IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Administrative Console	Yes	This console provides the connection to the ISE appliance for administration and management. The console can connect directly to ISE or over the network via a browser or SSHv2 connection. The TOE supports the following browsers: Firefox 18.x Firefox 15.x Firefox 14.x Firefox 9.x Firefox 8.x Firefox 5.x Internet Explorer 8.x Internet Explorer 9.x (IE8 Compatible Mode)
NTP Server(s)	No	The TOE supports communications with up to three NTP servers. Connection with an NTP server is to maintain an accurate time and synchronize time across different time zones. This procedure ensures that the logs provide a reliable timestamp. By having multiple NTP servers configured the time to converge when one of the NTP servers goes down is reduced. Because of the importance of reliable time in a security product, it is advised that multiple NTP servers are configured for ISE.
Remote Authentication Store	No	The TOE supports local authentication or authentication via a remote authentication store, including LDAP and Active Directory.
Syslog Target	Yes	The TOE must offload syslogs to an external entity, which can be another iteration of ISE or a syslog server that supports TLS-protected transfer.

5 Security Policy

5.1 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 authorized administrative user, and other system events.

The TOE can be configured to send syslog events to other devices, including other iterations of ISE, using a TLS protected collection method. Logs are classified into various predefined categories. The TOE also provides the capability for the administrator to customize the logging output by editing the categories with respect to their targets, severity level, etc. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted only to the authorized administrator, who has no access to edit them, only to copy or delete (clear) them.

The logs can be viewed by using the Operations -> Reports page on the ISE administration interface, then select the log from the left side and individual record (message). 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.

5.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The TOE relies on FIPS PUB 140-2 validation for testing of cryptographic functions, including self-tests and key zeroization. ISE uses Cisco Common Cryptographic Module (C3M) (FIPS 140-2 Cert#1643) and Cisco Secure Access Control Server (ACS) and FIPS module Network Services (NSS) (FIPS 140-2 Cert#1497). The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; cryptographic hashing using SHA1 (and other sizes); and keyed-hash message authentication using HMAC-SHA (multiple key sizes). The TOE supports SSH and TLS/HTTPS secure protocols.

5.3 User Data Protection

The TOE ensures that packets transmitted from the TOE do not contain residual information from previous packets. Packets that are not the required length use zeros, fixed data based on the amount of padding, or random data, for padding. Residual data is never transmitted from the TOE.

5.4 Identification and Authentication

All users wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services. Once a user attempts to access the management functionality of the TOE, the TOE prompts the user for a user name and password. 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 in order to perform the association of the credentials to an ISE Role Based Access Control role. For the SSH public key authentication method, the public keys configured by the EXEC CLI command "crypto key import" command will be used for signature verification. The user information is from the local user database. In all cases only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks. 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.

5.5 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:

- Enable, disable, determine and modify the behavior of the audit trail management
- Configure the cryptographic services
- Update the TOE and verify the updates via a hash comparison
- Enable, disable, determine and modify the behavior of communication of authorized external IT entities with the TOE
- Query, modify, delete, and assign the user attributes
- Specify the time limits of session inactivity

All of these management functions are restricted to the authorized administrator of the TOE, which covers all administrator roles (see table for FMT_SMR.2 in Section 6.1). The Authorized Administrators of the TOE are individuals who manage specific type of administrative tasks. The Authorized 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 Cisco ISE user interface provides an integrated network administration console from which you can manage various identity services. These services include authentication, authorization, posture, guest, profiler, as well as monitoring, troubleshooting, and reporting. All of these services can be managed from a single console window called the Cisco ISE dashboard. The navigation tabs and menus at the top of the window provide point-and-click access to all other administration features. A Command Line Interface (CLI) is also supplied for additional administration functionality. This interface can be used remotely over SSHv2.

5.6 Protection of the TSF

The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE and is able to detect modification of information and/or operations. The TOE also 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, or an NTP server (or servers) can be used to synchronize the date-timestamp. The TOE is also capable of ensuring software updates are from a reliable source. Finally, the TOE performs testing to verify correct operation.

In order for updates to be installed on the TOE, an administrator must use the provided hash value to confirm the integrity of the product.

5.7 TOE Access

The TOE can terminate inactive sessions after an authorized 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.

5.8 Trusted Path/Channels

The TOE establishes a trusted path between the ISE and the administrative web-based 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 using TLS and other external authentication stores using TLS-protected communications.

6 Documentation

The vendor provides guidance documentation on their support website, http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_common_criteria.html. The following documentation located on their support website was used as evidence for the evaluation of the Cisco Identity Services Engine (ISE):

- *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0*

There are many documents available on the support website, but the above mentioned document is the only one that is to be trusted as having been part of the evaluation. This guidance document contains the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance document is applicable for all models of the ISE product claimed by this evaluation. Additionally, the guidance document contains references and pointers to other TOE guidance documentation for additional detail regarding the security-related functionality. These references were also examined during the evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Cisco Identity Services Engine (ISE) running the software version 1.2, with patch 5 (1.2.0.899-5). This includes the ISE models 3415, 3495, and Virtual Machine, and their associated components defined in Table 2.

To use the product in the evaluated configuration, the product must be configured as specified in the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0* document. Refer to Section 6 for information on where to retrieve the document from Cisco's support website and how to use this document to configure the TOE into the evaluated configuration.

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 *Evaluation Technical Report for a Target of Evaluation "Cisco Identity Services Engine (ISE)" Evaluation Technical Report v3.0 dated January 21 2014*, which is not publically available.

8.1 Test Configuration

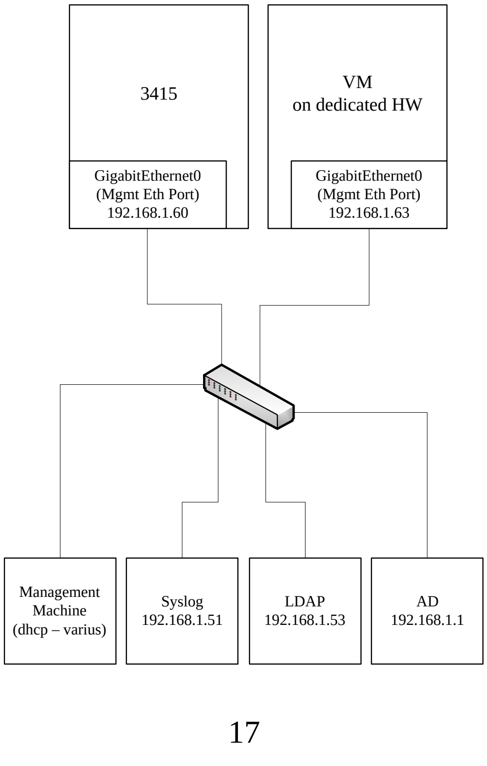
The evaluation team configured each model of the TOE according the *Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0* document for testing.

The following environment components and test tools* were utilized during the testing:

- Syslog Server: rsyslog 5.8.6-1ubuntu8.1 (note: this is an extension to sysklogd 1.5-6ubuntu1) was used for testing
- NTP Server: ntp_4.2.6.p3+dfsg-1ubuntu3.1_i386
- Active Directory: Windows Server 2008 R2 Enterprise Version 6.1 (Build 7601: Service Pack 1)
- LDAP: openldap 2.4.28-1.1ubuntu4.3
- Putty client: version .60
- WireShark: version 1.10.0
- Bitvise SSH Client: version 4.60

*Only the test tools utilized for functional testing have been listed.

The following figure depicts the configuration for the test environment that was utilized during the execution of the testing:



8.2 Developer Testing

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

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of the Cisco Identity Services Engine (ISE) by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. Each TOE external interface is to be described in the relevant design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, Functional Specification (FSP) and the independent test plan were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDPP for all *security relevant* TOE external interfaces. TOE external interfaces that will be determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Vulnerability Scanner (Burp Suite)
  This test used the Burp Suite Vulnerability Scanner to the TOE's web applications for vulnerabilities. The scanner probes a wide range of vulnerabilities that includes but is not limited to cross-site scripting, SQL injection, directory traversal, and unchecked file uploads as well as less critical vulnerabilities such as unnecessary information disclosure.
- Malformed Packet Flooding
  This attack attempts to exercise the stability of the IP stack and its components by sending a large amount of TCP packets and malformed TCP packets in an attempt to overload the application. If successful, the TOE will crash and not allow any connections until the TOE is rebooted.
- OpenSSH User Enumeration (Timing Attack)
  In this test, the attacker measures the time it takes for the server to respond to a request for a valid user vs. a request for an invalid user. Using consistencies and patterns in the time differences of valid vs. invalid user logon attempts, the attacker can brute-force enumerate valid SSH usernames.

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 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Identity Services Engine (ISE) TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 Identity Services Engine (ISE) product 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 Security Requirements for Network Devices Protection Profile (NDPP).

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 EAL 1 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 as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

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

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 1 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 NDPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, 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 EAL 1 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 EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator 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 NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

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 addressed the vulnerability analysis Assurance Activities in the NDPP, 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 NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the ISE being configured for FIPS operation. The validation team cautions the users that in order for the remote administrative sessions to operate within the specified cryptologic parameters, it is the remote CLIENT that must be configured to use the proper cryptographic algorithms.

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

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Cisco Identity Services Engine (ISE) Security Target, Version 1.0, January 2014*.

13 List of Acronyms

Acronym	**Definition**
AAA	Administration, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
IT	Information Technology
NAC	Network Access Control
NTP	Network Time Protocol
OS	Operating System
OSP	Organizational Security Policies
PP	Protection Profile
pp_nd_v1.1	U.S. Government Protection Profile, Security Requirements for Network Devices (NDPP)
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
SGA	Security Group Access
SGACL	Security Group Access Control List
SGT	Security Group tags
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VPN	Virtual Private Network
WLC	Wireless LAN Controller

14 Terminology

Terminology	Definition
Endpoints	An endpoint role is a set of permissions that determine the tasks that the device can perform or services that can be accessed on the Cisco ISE network. Endpoints can be users, personal computers, laptops, IP phones, printers, or any other device supported on the ISE network
Inline Posture node	A gate-keeping node that is positioned behind the network access devices. Inline Posture enforces access policies after a user has been authenticated and granted access. There can be or two maximum nodes instances running as Inline Posture node. The Inline Posture node cannot assume any other persona, due to its specialized nature.
Group member	A group member role is a set of permissions that determine the tasks a user (by virtue of being a member of a group) can perform or the services that can be accessed on the ISE network.
Node	A node is an individual instance of ISE. There are two types of nodes, an ISE node that can take on one of three Personas and the Inline Posture node.
Node type	The TOE can be one of two types; an ISE node or an Inline posture node. The node type and persona determine the type of functionality provided by the node.
Persona	The persona of a node determines that service provided by a node. The TOE can be configure as any of the following personas: • Administration – allows the user to perform all of the administrative operations on the TOE. All of the authentication, authorization, auditing, and so on are managed. There can be one or two maximum node instances running the Administration persona and can take any one of the following roles; standalone, primary, or secondary. • Policy Service – provides network access, posture, guest services, client provisioning, and profiling services. This persona evaluates the policies and makes all of the decisions. There can be one or more instance of a node configured as a Policy Service. • Monitoring – functions as the log collector and stores log messages from all of the Administration and Policy Service personas. There can be one or two node instances running the Monitoring persona.
Role	The role identity determines of the TOE is a standalone, primary, or secondary node.
Service	A service is a specific feature that a persona provides, such as network access, posture, security group access, and monitoring
User	A user role is a set of permissions that determine what tasks a user can perform or what services can be accessed on the ISE network. The user identity includes username, password, and group association.

15 Bibliography

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) Security Target, Version 1.0, January 2014.
6. Evaluation Technical Report for a Target of Evaluation “Cisco Identity Services Engine (ISE)” Evaluation Technical Report v3.0 dated January 21 2014.
7. Cisco Identity Services Engine (ISE) Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0