# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# for

# Cisco Prime Infrastructure

| | |
|---|---|
| **Report Number:** | **CCEVS-VR-VID10860-2018** |
| **Dated:** | **April 30, 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

Daniel P Faigin
Marybeth S Panock

## Common Criteria Testing Laboratory

Swapna Katikaneni
Madelyn Lanoue

*CGI IT Security Labs*

# Table of Contents

1 Executive Summary ....................................1
2 Identification ....................................3
3 Architectural Information ....................................4
4 Assumptions, Threats, and Scope ....................................5
4.1 Assumptions ....................................5
4.2 Threats ....................................6
4.3 Clarification of Scope ....................................8
5 Security Policy ....................................9
5.1 Security Audit ....................................9
5.2 Cryptographic Support ....................................9
5.3 Identification and Authentication ....................................9
5.4 Security Management ....................................9
5.5 Protection of the TSF ....................................9
5.6 TOE Access ....................................10
5.7 Trusted path/Channels ....................................10
6 Documentation ....................................11
7 Independent Testing ....................................12
8 Evaluated Configuration ....................................14
9 Results of the Evaluation ....................................15
9.1 Evaluation of the Security Target (ASE) ....................................15
9.2 Evaluation of the Development (ADV) ....................................15
9.3 Evaluation of the Guidance Documents (AGD) ....................................15
9.4 Evaluation of the Life Cycle Support Activities (ALC) ....................................15
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) ....................................16
9.6 Vulnerability Assessment Activity (VAN) ....................................16
9.7 Summary of Evaluation Results ....................................16
10 Validator Comments/Recommendations ....................................17
11 Annexes ....................................18
12 Security Target ....................................19
13 Abbreviations and Acronyms ....................................20
14 Bibliography ....................................21

# List of Tables

Table 1: Platform in the Evaluated Configuration ........ 1
Table 2: Evaluation Details ........ 2
Table 3: ST and TOE Identification ........ 3
Table 4: Assumptions ........ 5
Table 5: Threats ........ 6
Table 6: Supporting TOE Guidance Documentation ........ 11
Table 7: Test Configuration Components and Tools Information ........ 13
Table 8: Required IT Environment Components ........ 14

# List of Figures

Figure 1: TOE Deployment Example ........ 4
Figure 2: Cisco Systems TOE Environment Setup ........ 12

# 1 Executive Summary

This report 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 in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 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 Cisco Prime Infrastructure (hereafter referenced as Cisco PI). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (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 as documented in the ST.

The evaluation of Cisco PI was performed by CGI IT Security Labs in Fairfax, Virginia, in the United States and was completed in April 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in collaborative Protection Profile for Network Devices (NDcPP) v1.0. The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The CGI ITSL evaluation team determined that Cisco PI is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST.

The Cisco Prime Infrastructure TOE is a network management product comprised of hardware and software. The physical boundary of the TOE is described in 1 below

| | |
|---|---|
| **Hardware** | Cisco Prime Infrastructure Physical Appliance (Gen 2)<br>○ Product ID: PI-UCS-APL-K9<br>○ Hardware model: Cisco UCS-C220–M4<br>○ Processor: Dual Intel® Xeon E5-2650 v3 @2.30GHz 8 core processor<br>○ Memory: 64 GB<br>○ Hard Disk: 4 x 900GB RAID10<br>○ NIC: Integrated dual-port Gigabit Ethernet |
| **Software** | Cisco Prime Infrastructure 3.2-FIPS Physical Appliance ISO image with PI-patch-fips-1 |

**Table 1: Platform in the Evaluated Configuration**

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PP had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the 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.

**Table 2: Evaluation Details**

| **Item** | **Identifier** |
|---|---|
| **Evaluated Product** | Cisco Prime Infrastructure |
| **PP** | collaborative Protection Profile for Network Devices (NDcPP) v1.0. |
| **ST** | Cisco Prime Infrastructure, Version 1.3, April 25, 2018 |
| **ETR** | Evaluation Technical Report for Cisco Prime Infrastructure, Version 1.0, April 27, 2018 |
| **Sponsor & Developer** | Cisco Systems, Inc.<br>170 West Tasman Drive<br>San Jose, CA 95134 |
| **CCTL** | CGI IT Security Labs<br>12601 Fair lakes Circle<br>Fairfax, VA 22033 |
| **Completion Date** | April 2018 |
| **CC** | Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 |
| **CEM** | Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012 |
| **Disclaimer** | The information contained in this Validation Report is not an endorsement of the Cisco Prime Infrastructure by any agency of the U.S. Government and no warranty is either expressed or implied. |
| **Evaluation Personnel** | Swapna Katikaneni<br>Madelyn Lanoue |
| **Validation Personnel** | Daniel P Faigin<br>Marybeth S Panock |

# 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) 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 Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

**Table 3: ST and TOE Identification**

| Name | Description |
|---|---|
| ST Title | Cisco Prime Infrastructure |
| ST Version | 1.3 |
| Publication Date | April 25, 2018 |
| Vendor and ST Author | Cisco Systems, Inc. |
| TOE Reference | Cisco Prime Infrastructure |
| TOE Hardware Models | Cisco Prime Infrastructure Physical Appliance (Gen 2) |
| TOE Software Version | Cisco Prime Infrastructure 3.2-FIPS Physical Appliance ISO image with PI-patch-fips-1 |
| Keywords | Network Management |

# 3 Architectural Information

The Cisco Prime Infrastructure 3.2-FIPS TOE is a network management product comprised of hardware and software. The following figure provides a simplified visual depiction of an example TOE deployment.

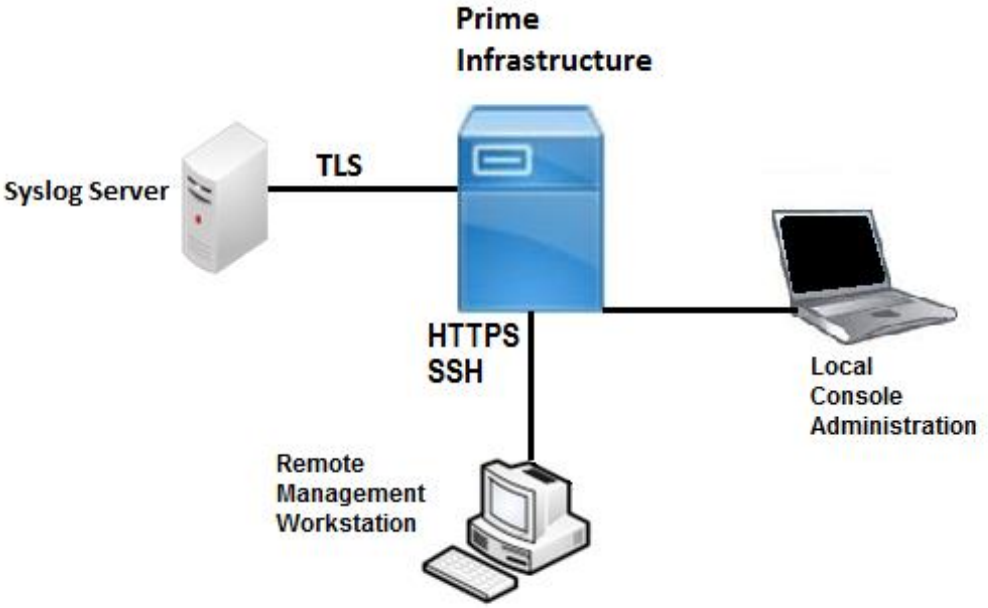

**Figure 1: TOE Deployment Example**

# 4 Assumptions, Threats, and Scope

## 4.1 Assumptions

The ST identifies the following assumptions about the use of the product:

**Table 4: 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 ND cPP. 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. |
| A.REGULAR_UPDATES | The network device firmware and software is assumed to be updated by an administrator on a regular basis in |

| Assumption | Assumption Definition |
|---|---|
| | 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. |

## 4.2 Threats

The ST identifies the following threats that the TOE and its operational environment are intended to counter:

**Table 5: 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. |
| 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. |

| Threat | Threat Definition |
|---|---|
| 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. |
| 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. |

| Threat | Threat Definition |
|---|---|
| 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. |

## 4.3 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:

1. 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 claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific device models and software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. 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.

# 5 Security Policy

The TOE enforces the following security policies as described in the ST.

## 5.1 Security Audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE 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, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are transmitted to an external audit server over an encrypted channel.

## 5.2 Cryptographic Support

The TOE implements cryptography and algorithms that has been CAVP tested. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation.

## 5.3 Identification and Authentication

The TOE performs two types of authentication to provide a trusted means for Security Administrators and remote endpoints to interact with itself: X.509v3 certificate-based authentication for remote devices and password-based authentication for Security Administrators. Device-level authentication allows the TOE to establish a secure communication channel with a remote endpoints.

Security Administrators have the ability to compose strong passwords (15 characters or greater), which are stored in a hashed form.

## 5.4 Security Management

The TOE provides secure remote administrative interface and a local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity time before session termination as well as an ability to update its software.

The TOE provides a Security Administrator role and only the Security Administrator can perform security management functions.

## 5.5 Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE also provides reliable timestamps to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides a trusted software update and verification function to assure software updates are from Cisco Systems, Inc.

## 5.6 TOE Access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate. The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

## 5.7 Trusted path/Channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

In addition the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

# 6 Documentation

Cisco offers a number of guidance documents along with a CC-specific supplemental document describing the installation process for the TOE as well as guidance for subsequent use and administration of the applicable security features.

The guidance documentation examined during the course of the evaluation and delivered with the TOE is as follows:

- Cisco Prime Infrastructure 3.2 Common Criteria Configuration Guide, Version 0.7, April 25, 2018

This document in turn references the following documents that provide additional detailed guidance for specific TOE capabilities. Note that the evaluation examined these referenced documents only to the extent necessary to complete the assurance activities specified in the claimed PPs.

**Table 6: Supporting TOE Guidance Documentation**

| # | Title | Link |
|---|---|---|
| [1] | Cisco Prime Infrastructure 3.2 Appliance Hardware Installation Guide | http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/hardware_install/guide/Cisco_PI_Hardware_Appliance_Installation_Guide/cpiInstallUCS.html |
| [2] | Cisco Prime Infrastructure 3.2 Quick Start Guide | http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/quickstart/guide/cpi_qsg.html |
| [3] | Cisco Prime Infrastructure 3.2 Administrator Guide | http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/admin/guide/bk_CiscoPrimeInfastructure_3_2_AdminGuide.html |
| [4] | Cisco Prime Infrastructure 3.2 User Guide | http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/user/guide/bk_CiscoPrimeInfrastructure_3_2_0_UserGuide.html |
| [5] | Cisco Prime Infrastructure 3.2 Command Reference Guide | https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/command/reference/cli32/cli312_appendix_011.html |
| [6] | Cisco Prime Infrastructure 3.2 Release Notes | http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/release/notes/cpi_rn.html |

The above documents are considered to be part of the evaluated TOE. Any additional customer documentation delivered with the TOE or made available through electronic downloads should not be relied upon for using the TOE in its evaluated configuration.

The Security Target used is:

- Cisco Prime Infrastructure Security Target

# 7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- Independent Test Plan and Report for Cisco Prime Infrastructure, Version 1.1, April 26, 2018

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report for Cisco Prime Infrastructure, Version 1.1, April 27, 2018

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices (NDcPP) v1.0. Independent testing took place at the CGI ITSL location in Fairfax, Virginia.

Figure 2 below depicts a diagram of the test environment with a list of tools used by the evaluators. The Network Components and Software are shown in Table 7, following.

**Figure 2: Cisco Systems TOE Environment Setup**

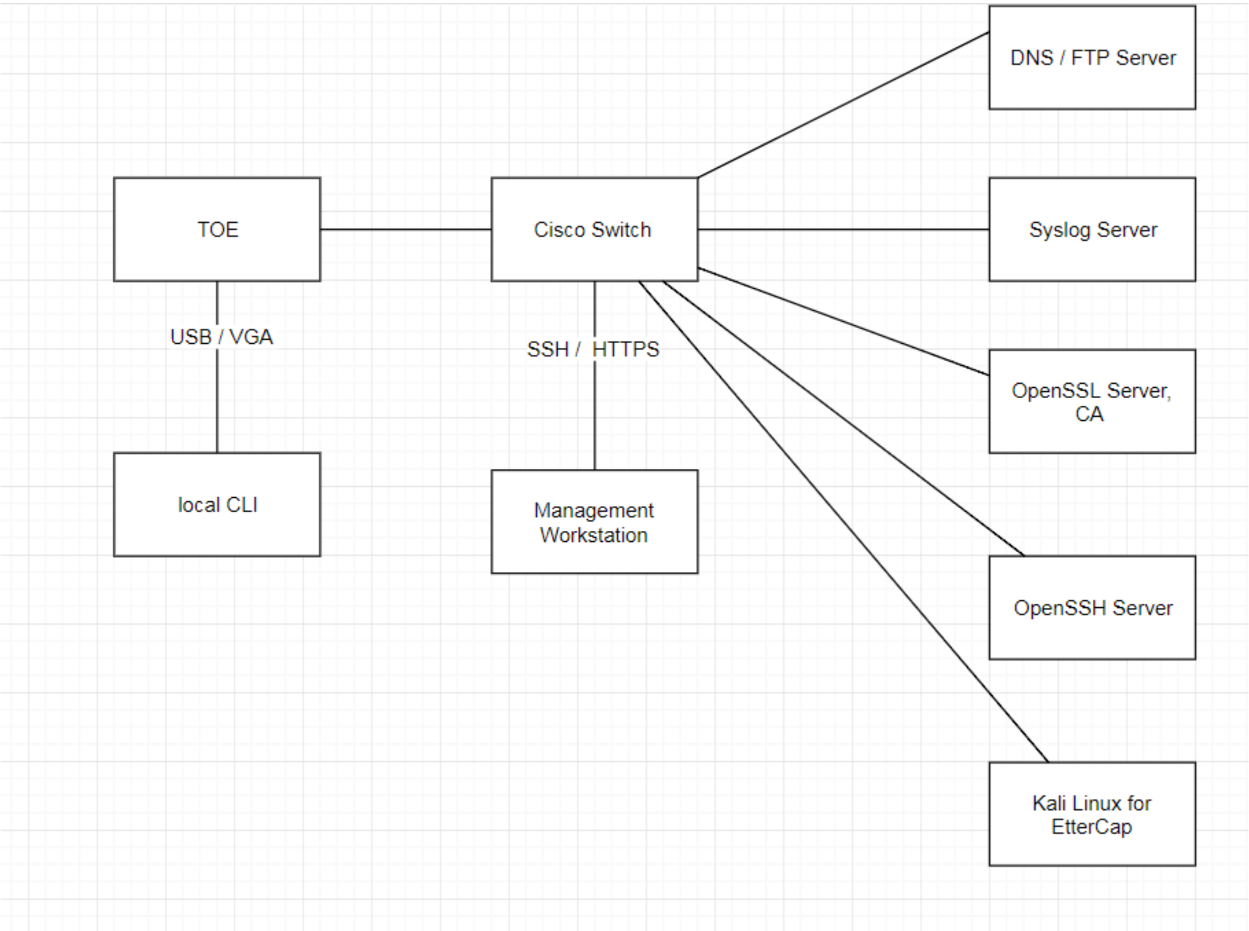

**Table 7: Test Configuration Components and Tools Information**

| Test Network Component | Software |
|---|---|
| Cisco Catalyst Switch 3750X | Cisco IOS 15.0(2) SE4 |
| Syslog-ng | syslog-ng PE-7.0.7 |
| OpenSSH Server | OpenSSH-6.9p1 |
| CA Server, OpenSSL Server | OpenSSL-1.1.0d |
| DNS Server | N/A |
| Management Workstation | Wireshark, Puttygen, Putty, Windows 7 |

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the collaborative Protection Profile for Network Devices (NDcPP) v1.0 have been fulfilled.

# 8 Evaluated Configuration

The evaluated version of the TOE is running Cisco Prime Infrastructure 3.2-FIPS Physical Appliance ISO image with PI-patch-fips-1, as installed and configured according to the CC Configuration Guide as well as the supporting guidance documentation identified in Table 6.

The TOE evaluated configuration requires the following components shown in Table 8 below.

**Table 8: Required IT Environment Components**

| Component | Usage/Purpose Description |
|---|---|
| Management Workstation | This includes:<br>o A Mac or Windows laptop or desktop with one of the following web browsers supporting TLS v1.2:<br>▪ Google Chrome 59 or later<br>▪ Microsoft Internet Explorer 11 (No plug-ins are required.)<br>▪ Mozilla Firefox ESR 52<br>▪ Mozilla Firefox 56 or later<br>o A Mac, UNIX, or Windows laptop or desktop with a SSH v2 client |
| Local Console | This includes any IT Environment Console that is directly connected to the TOE component via the Serial Console Port and supports a baud rate of 9600 bits per second. |
| Syslog Server | This includes any syslog server that can be accessed over TLS v1.2 with the supported ciphersuites. |

# 9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in collaborative Protection Profile for Network Devices (NDcPP) v1.0, in conjunction with version 3.1, revision 4 of the CC and the CEM.

Examinations were performed on the Security Target, Development documentation, Test Documentation, and Guidance documentation. The validation team also performed an assessment on the evaluation lab's Assurance Activities Report.

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 claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the CGI ITSL.

## 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 PI product 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 PP 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 PP 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 proprietary Penetration Test Report prepared by the evaluator, and summarized in the AAR. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include:

1. Cisco UCS-C220–M4
2. Cisco Prime Infrastructure Physical Appliance (Gen 2)
3. Cisco Prime Infrastructure 3.2-FIPS
4. Cisco PI 3.2
5. Cisco ADE-OS version 3.1.0.001
6. Dual Intel® Xeon E5-2650 v3 @2.30GHz 8 core processor
7. Cisco TLS 1.2
8. Cisco SSH v2
9. TCP

The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor.

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 functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the Cisco PI that are outside the scope of NDcPP v1.0, are not covered by this evaluation, need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

On the GUI interface, the names and versions of installed software are listed before login. As this is a concern in some contexts, the validation team investigated the concern and determined it did not require addressing, is it is available only over a secured channel.

# 11 Annexes

Not applicable.

# 12 Security Target

Cisco Prime Infrastructure Security Target Version 1.3, April 25, 2018

# 13 Abbreviations and Acronyms

| | |
|---|---|
| **AAA** | Authentication, Authorization and Accounting |
| **AAR** | Assurance Activities Report |
| **CAVP** | Cryptographic Algorithm Validation Program |
| **CC** | Common Criteria |
| **CCEVS** | Common Criteria Evaluation and Validation Scheme |
| **CCTL** | CC Testing Laboratory |
| **CEM** | Common Methodology for IT Security Evaluation |
| **CLI** | Command Line Interface |
| **EP** | Extended Package |
| **ESP** | Encapsulating Security Payload |
| **ETR** | Evaluation Technical Report |
| **FIPS** | Federal Information Processing Standard |
| **IT** | Information Technology |
| **LAN** | Local Area Network |
| **NDcPP** | Collaborative Network Device Protection Profile |
| **NIAP** | National Information Assurance Partnership |
| **NIST** | National Institute of Standards and Technology |
| **NSA** | National Security Agency |
| **NTP** | Network Time Protocol |
| **NVLAP** | National Voluntary Laboratory Assessment Program |
| **OS** | Operating System |
| **PCL** | Product Compliant List |
| **PP** | Protection Profile |
| **RFC** | Request For Comment |
| **SAR** | Security Assurance Requirement |
| **SFR** | Security Functional Requirement |
| **SNMP** | Simple Network Management Protocol |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functions |
| **TSS** | TOE Summary Specification |
| **VR** | Validation Report |

# 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, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] Cisco Prime Infrastructure Security Target Version 1.3, April 25, 2018

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.

[7] Evaluation Technical Report for Cisco Prime Infrastructure Version 1.0, April 27, 2018.

[8] Assurance Activities Report for Cisco Prime Infrastructure Version 1.1, April 27, 2018