National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015

Report Number: CCEVS-VR-PP-0028
Dated: 07 April 2016
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

Common Criteria Testing Laboratory

Protection Profile Evaluation
Booz Allen Hamilton.
Linthicum, 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 the Collaborative Protection Profile for Network Devices, Version 1.0 (NDcPP1.0). It presents a summary of the NDcPP1.0 and the evaluation results.

The evaluation of the NDcPP1.0 was performed against the APE class Security Assurance Requirements (SARs) defined in CC Part 3 [3] and the Common Evaluation Methodology (CEM) [4]. The evaluation was performed by the Booz Allen Hamilton (BAH) Common Criteria Testing Laboratory (CCTL) in Linthicum, Maryland, United States of America, and was completed in February 2016.

An evaluation of the NDcPP1.0 was also performed concurrent with the first product evaluation against the PP's requirements. This evaluation supplemented the BAH evaluation to account for optional requirements within the NDcPP1.0. In this case the Target of Evaluation (TOE) was the Cisco Catalyst 3K/4K Wired Access Switches running IOS-XE 3.8.0E. The evaluation was performed by the Gossamer Security Solutions Common Criteria Testing Laboratory (CCTL) in Catonsville, Maryland, United States of America, and was completed in March 2016. During the evaluation, a few interpretation issues were raised to the NIAP Technical Rapid Response Team. These issues were addressed and forwarded to the Network iTC Interpretation Team (NIT) for future NDcPP revisions but did not result in any PP deficiencies.

Both evaluations determined that the NDcPP1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. The PP 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).

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 found that the evaluation showed that the NDcPP1.0 meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced, resulting in a fully conformant cPP.

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). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

The NDcPP1.0 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either conditional or strictly optional, depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, and the subsequent evaluation that addresses additional optional requirements in the NDcPP1.0.

Protection Profile	*Collaborative Protection Profile for Network Devices, version 1.0, February 27, 2015*
ST Evaluation	*Cisco Catalyst 3K/4K Wired Access Switches Common Criteria Security Target, Version 1.0, March 04, 2016 (including the optional audit and IPsec requirements).*
Evaluation Technical Report	*Evaluation Technical Report for Cisco Catalyst 3K/4K Wired Access Switches, Version 1.1, March 04, 2016*
CCTL	*Gossamer Security Solutions, Inc., Catonsville, MD*
CCEVS Validators	*Paul Bicknell, Lisa Mitchell, Chris Thorpe – The MITRE Corporation*
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 extended
CCTL (APE Eval)	Booz Allen Hamilton, Linthicum, MD USA

3 NDcPP Description

This Protection Profile focuses on the security functionality of network devices. A network device in the context of the NDcPP1.0 is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network.

The aim is that any network device that meets the NDcPP1.0 will "behave" on the network and can be trusted to do no harm. To accomplish this, the network device is expected to employ standards-based tunneling protocols to include IPsec, TLS, or SSH to protect the communication paths to external entities. It is also required that X.509 certificates be used for authentication purposes; use of certificates is supported as an option for code signing/digital signature services.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational 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 1: TOE Assumptions

Assumption Name	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.
A.REGULAR_UPDATES	The network device firmware and software is assumed

Assumption Name	Assumption Definition
	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.

4.2 Threats

Table 2: Threats

Threat Name	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.
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

Threat Name	Threat Definition
	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.
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 Organizational Security Policies

The following table contains organizational security policies defined for the TOE.

Table 3: Organizational Security Policies for the TOE

TOE Security Obj.	TOE Security Objective Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Security Objectives

The following table contains objectives for the Operational Environment.

Table 4: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	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.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

5 Requirements

As indicated above, requirements in the NDcPP1.0 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the APE class evaluation.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Identity Association
	FAU_STG_EXT.1: Protected Audit Event Storage
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_CKM.4: Cryptographic Key Destruction
	FCS_COP.1(1): Cryptographic Operation – AES Data Encryption/Decryption
	FCS_COP.1(2): Cryptographic Operation – Signature Generation and Verification
	FCS_COP.1(3): Cryptographic Operation – Hash Algorithm
	FCS_COP.1(4): Cryptographic Operation – Keyed-Hash Algorithm
	FCS_RBG_EXT.1: Random Bit Generation
FIA: Identification and Authentication	FIA_PMG_EXT.1: Password Management
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UAU_EXT.2: Password-based Authentication Mechanism
	FIA_UAU.7: Protected Authentication Feedback
	FIA_X509_EXT.1: X.509 Certificate Validation
	FIA_X509_EXT.2: X.509 Certificate Authentication
	FIA_X509_EXT.3: X.509 Certificate Requests
FMT: Security	FMT_MOF.1(1): Management of Security Functions Behavior

Requirement Class	Requirement Component
Management	FMT_MTD.1: Management of TSF Data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.2: Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1: Protection of Administrator Passwords
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Trusted Update
	FPT_STM.1: Reliable Time Stamps
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

The following table contains the optional requirements contained in NDcPP v1.0, Appendices A and B, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG.1: Protected Audit Trail Storage	Cisco Catalyst 3K/4K Wired Access Switches Common Criteria Security Target, 4 March 2016
	FAU_STG_EXT.2: Counting Lost Audit Data	PP Evaluation
	FAU_STG_EXT.3: Display Warning for Local Storage Space	PP Evaluation
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS Protocol	PP Evaluation
	FCS_IPSEC_EXT.1: IPsec Protocol	Cisco Catalyst 3K/4K Wired Access Switches Common Criteria Security Target, 4 March 2016
	FCS_SSHC_EXT.1: SSH Client Protocol	PP Evaluation
	FCS_SSHS_EXT.1: SSH Server Protocol	PP Evaluation
	FCS_TLSC_EXT.1: TLS Client Protocol	PP Evaluation
	FCS_TLSC_EXT.2: TLS Client Protocol with authentication	PP Evaluation
	FCS_TLSS_EXT.1: TLS Server Protocol	PP Evaluation
	FCS_TLSS_EXT.2: TLS Server Protocol with mutual authentication	PP Evaluation
FMT: Security Management	FMT_MOF.1(1)/Audit: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(2)/Audit: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(1)/AdminAct: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(2)/AdminAct: Management of Security Functions Behavior	PP Evaluation

Requirement Class	Requirement Component	Verified By
	FMT_MOF.1/LocSpace: Management of Security Functions Behavior	PP Evaluation
	FMT_MOF.1(2)/TrustedUpdate: Management of Security Functions Behavior	PP Evaluation
	FMT_MTD.1/AdminAct: Management of TSF Data	PP Evaluation
FPT: Protection of the TSF	FPT_FLS.1/LocSpace: Failure with Preservation of Secure State	PP Evaluation
	FPT_TST_EXT.2: Self tests based on certificates	PP Evaluation
	FPT_TUD_EXT.2: Trusted Update based on certificates	PP Evaluation

6 Assurance Requirements

The following are the assurance requirements contained in the NDcPP1.0:

Requirement Class	Requirement Component
ASE: Security Target	ASE_CCL.1: Conformance Claims
	ASE_ECD.1: Extended Components Definition
	ASE_INT.1: ST Introduction
	ASE_OBJ.1: Security Objectives for the Operational Environment
	ASE_REQ.1: Stated Security Requirements
	ASE_SPD.1: Security Problem Definition
	ASE_TSS.1: TOE Summary Specification
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the Evaluation

The CCTL reviewed the NDcPP1.0 to derive the following initial results.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

The PP was found to pass all applicable APE assurance requirements.

8 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 as interpreted by the supplemental guidance in the ESMICMPP Assurance Activities to determine whether or not the claims made are justified.
- **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.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Collaborative Protection Profile for Network Devices, version 1.0, February 27, 2015.

[7] Cisco Catalyst 3K/4K Wired Access Switches Common Criteria Security Target, Version 1.0, March 04, 2016 (including the optional Audit and IPsec requirements).

[8] Evaluation Technical Report for Cisco Catalyst 3K/4K Wired Access Switches, Version 1.1, March 04, 2016