National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Security Requirements for Network Devices, Version 1.0

Report Number: **CCEVS-VR-PP-0002**
Dated: **31 January 2014**
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

Base and Additional Requirements
Leidos (formerly SAIC)
Columbia, 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 Security Requirements for Network Devices (version 1.0) Protection Profile, also referred to as the Network Device Protection Profile (NDPP). It presents a summary of the NDPP and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the NDPP was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Cisco Catalyst Switches 3560C, 3560X, and 3750X running IOS 15.0.(2)SE4 (subsequently referred to as Cisco Catalyst 3K Switches) provided by Cisco Systems, Inc. The evaluation was performed by the Leidos (formerly SAIC) CCTL in Columbia, Maryland, USA, and was completed in January 2014. This evaluation addressed the base requirements as well as additional requirements in Appendix C of the NDPP.

The information in this report is largely derived from the Evaluation Technical Report (ETR) written by the Leidos (formerly SAIC) CCTL.

The evaluation determined that the NDPP is both **Common Criteria Part 2 Extended and Part 3 Conformant**. 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 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). Because the ST contains only material drawn directly from the NDPP, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

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 are consistent with the evidence provided.

The validation team found that the evaluation showed that the NDPP meets the requirements of the APE components. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the NDPP was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Cisco Catalyst 3K Switches provided by Cisco Systems, Inc.

The evaluation was performed by the Leidos (formerly SAIC) CCTL in Columbia, Maryland, USA, and was completed in January 2014.

The NDPP contains a set of “base” requirements that all conformant STs must include, and in addition contain a set of “optional” requirements that may be included based on the selections made in the base requirements and the capabilities of the TOE. Because the optional requirements do not have to be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any optional requirements that are incorporated into the that initial ST. Subsequently, TOEs that are evaluated against the NDPP that incorporate optional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and the appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the NDPP.

Protection Profile	*Security Requirements for Network Devices, Version 1.0, 10 December 2010*
ST (Base)	Cisco Catalyst Switches (3560C, 3560X and 3750X) Running IOS 15.0(2)SE4, Version 1.0, January 16, 2014
Evaluation Technical Report (Base)	Evaluation Technical Report For the Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0.(2)SE3, Version 1.0, August 16, 2013
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (Base)	Leidos (formerly SAIC), Columbia, MD
CCEVS Validators	Ken Elliott, The Aerospace Corporation

3 NDPP Description

The NDPP describes security requirements for a network device. A network device in the context of the PP is a device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise. Examples of a “network device” that should claim compliance to the PP include routers, firewalls, IDSs, audit servers, and switches that have Layer 3 functionality. Examples of devices that connect to a network but are not suitable for evaluation against the PP include mobile devices (“smart phones”), end-user workstations, SQL servers, web servers, application servers, and database servers.

Compliant TOEs will provide security functionality that addresses threats to the TOE and implements policies that are imposed by law or regulation. Compliant TOEs must protect communications to and between elements of a distributed TOE (e.g., between a network IDS sensor and the centralized IDS manager) or instantiations of the TOE in a single enterprise (e.g., between routers). The TOE must offer identification and authentication services that support the composition of moderate complex passwords or passphrases, and make these services available locally (that is, a local logon) as well as remotely (remote login). The TOE must also offer auditing of a set of events that are associated with security-relevant activity on the TOE, although these events will be stored on a device that is distinct from the TOE. The TOE must offer some protection for common network denial of service attacks and must also provide the ability to verify the source of updates to the TOE.

While the protocols required by the PP make use of certificates, the PP does not levy requirements on the certificate infrastructure (for example, using OCSP to verify a certificate's validity).

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.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
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

Threat Name	Threat Definition
	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.

4.3 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs.

Table 3: Organizational Security Policies

Policy Name	Policy 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 for the TOE

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
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

TOE Security Obj.	TOE Security Objective Definition
	resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
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.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
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.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Requirements

As indicated above, requirements in the NDPP are comprised of the “base” requirements (appearing in Section 4.2) and additional requirements appearing in Appendix C of the NDPP. The following are table contains the “base” requirements that were validated as part of the HP A Series evaluation activity referenced above.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User identity association
	FAU_STG_EXT.1: External Audit Trail Storage
	FAU_STG_EXT.3: Action in case of Loss of Audit Server Connectivity
FCS: Cryptographic support	FCS_CKM.1: Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-

Requirement Class	Requirement Component
	hash message authentication)
	FCS_RBG_EXT.1: Extended: Cryptographic Operation (Random Bit Generation)
	FCS_COMM_PROT_EXT.1: Extended: Communications Protection
FDP: User data protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1: Password Management
	FIA_UAU.7: Protected Authentication Feedback
	FIA_UAU_EXT.5: Extended: Password-based Authentication Mechanism
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UAU.6: Re-authenticating
FMT: Security management	FMT_MTD.1: Management of TSF Data (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection (Disclosure)
	FPT_ITT.1(1) Basic Internal TSF Data Transfer Protection (Modification)
	FPT_PTD.1(1): Management of TSF Data (for reading of authentication data)
	FPT_PTD.1(20: Management of TSF Data (for reading of all symmetric keys)
	FPT_RPL.1: Replay Detection
	FPT_STM.1: Reliable Time Stamps
	FPT_TST_EXT.1: Extended: TSF Testing
	FPT_TUD_EXT.1: Extended: Trusted Update
FRU: Resource Utilization	FRU_RSA.1: Maximum Quotas
FTA: TOE access	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (Prevention of Disclosure)
	FTP_ITC.1(2): Inter-TSF Trusted Channel (Prevention of Modification)
	FTP_TRP.1(1): Trusted Path (Prevention of Disclosure)
	FTP_TRP.1(2): Trusted Path (Prevention of Modification)

The following table contains the “optional” requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the

Identification section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated.

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic support	FCS_IPSEC_EXT.1: Explicit: IPSEC	Cisco Cat 3 Switches, 31 January 2014
	FCS_TLS_EXT.1: Explicit: TLS	
	FCS_SSH_EXT.1: Explicit: SSH	
	FCS_HTTPS_EXT.1: Explicit: HTTPS	

6 Assurance Requirements

The following are the assurance requirements contained in the NDPP:

Requirement Class	Requirement Component
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 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

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

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 NDPP 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] Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4 Security Target, version 1.0, December 3, 2013

[7] Evaluation Technical Report for Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4, parts 1 and 2, version 1.0, August 2013

[8] *Security Requirements for Network Devices*, Version 1.0, 10 December 2010