National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Cisco Systems, Inc.

for

Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. 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 adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Date Issued: 2014-01-31

Validation Report Number: CCEVS-VR-VID10515-2014

CCTL: Leidos (formerly SAIC) Common Criteria Testing Laboratory

Assurance Level: PP Compliant

Protection Profile Identifier:
Protection Profile for Network Devices Version 1.0

Original Signed By

Acting Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency

National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

For

Cisco Catalyst Switches (3560C, 3560X, and 3750X) running IOS 15.0(2)SE4

Report Number: CCEVS-VR-VID10515-2014
Dated: January 31, 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

Table of Contents

1.1 Executive Summary 1
1.2 Evaluation Details 5
1.3 Identification 6
1.4 TOE Threats, Assumptions, and Organizational Security Policies 6
1.5 Architectural Information 6
1.6 Physical Boundaries 7
1.7 Documentation 8
1.8 Security Policy 8
1.9 Independent Testing 11
1.10 Evaluated Configuration 11
1.11 Results of the Evaluation 11
1.12 Validator Comments/Recommendations 12
1.13 Annexes 12
1.14 Security Target 12
1.15 Acronym List 13
1.16 Bibliography 13

List of Tables

Table 1 ST and TOE identification 6

1.1 Executive Summary

The evaluation of Cisco Catalyst Switches 3560C, 3560X, and 3750X running IOS 15.0.(2)SE4 (hereafter referenced as Cisco Cat 3k Switches) was performed by Leidos, in the United States and was completed in December 2013. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Cisco Cat 3k Switches TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 3.

Leidos Common Criteria Testing Laboratory determined that the product satisfies the evaluation assurance level (EAL) 1 as defined within the Common Criteria (CC) and the NDPP. The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the Cisco Catalyst Switches (3560C, 3560X, and 3750X) running IOS 15.0(2) SE4 Security Target, version 1.0, 16 January, 2014.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is Cisco Catalyst Switches (3560C, 3560X, and 3750X) running Cisco IOS 15.0(2)SE4 software.

The TOE hardware includes the following appliances:

1. Cisco Catalyst 3560C Switches

Figure 3: Cisco Catalyst 3560-C Series Switches

Table 3: Configurations of Cisco Catalyst 3560-C Series Switches

Catalyst 3560-C Switch Model	Description	PoE Output Ports and available PoE Power	Uplinks	MACsec
Cisco Catalyst 3560C-8PC-S	8 x 10/100 Fast Ethernet	8 PoE+, 124W	2 x 1G copper or 1G SFP	Yes

Catalyst 3560-C Switch Model	Description	PoE Output Ports and available PoE Power	Uplinks	MACsec
Cisco Catalyst 3560C-12PC-S	12 x 10/100 Fast Ethernet	12 PoE+, 124W	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560CG-8TC-S	8 x 10/100/1000 Gigabit Ethernet	N/A	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560CG-8PC-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE+, 124W	2 x 1G copper or 1G SFP	Yes
Cisco Catalyst 3560CPD-8PT-S	8 x 10/100/1000 Gigabit Ethernet	8 PoE, Up to 15.4W	2 x 1G (PoE+ input)	Yes

2. Cisco Catalyst 3560X Switches

Figure 4: The Cisco Catalyst 3560-X Series Configurations

Table 4: Configurations of Cisco Catalyst 3560-X Series Switches

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	WS-C3560-X-24T-L/Standalone	24	350W	-
	WS-C3560-X-48T-L/Standalone	48		
	WS-C3560-X-24P-L/Standalone	24 PoE+	715W	435W
	WS-C3560-X-	48 PoE+		

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	48P-L/Standalone			
	WS-C3560-X-48PF-L/Standalone	48 PoE+	1100W	800W
	WS-C3560-X-24T-S/Standalone	24	350W	-
	WS-C3560-X-48T-S/Standalone	48		
	WS-C3560-X-24P-S/Standalone	24 PoE+	715W	435W
	WS-C3560-X-48P-S/Standalone	48 PoE+		
	WS-C3560-X-48PF-S/Standalone	48 PoE+	1100W	800W

3. Cisco Catalyst 3750X Switches

Figure 5: The Cisco Catalyst 3750-X Series Configurations – Front and back view

Table 5: The Cisco Catalyst 3750-X Series Configurations

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	WS-C3760X-24T-L/Stackable (stackpower available with upgrade to IPBase)	24	350W	-

	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
	WS-C3760X-48T-L/Stackable	48		
	WS-C3760X-24P-L/Stackable	24 PoE+	715W	435W
	WS-C3760X-48P-L/Stackable	48 PoE+		
	WS-C3760X-48PF-L/Stackable	48 PoE+	1100W	800W
	WS-C3760X-24T-S/Stackable (stack power)	24	350W	-
	WS-C3760X-48T-S/Stackable	48		
	WS-C3760X-24P-S/Stackable	24 PoE+	715W	435W
	WS-C3760X-48P-S/Stackable	48 PoE+		
	WS-C3560-X-48PF-S/Stackable	48 PoE+	1100W	800W
	WS-C3750-X-12S-E/Stackable	12 GE SFP	350W	-
	WS-C3750-X-24S-E/Stackable	24 GE SFP	350W	

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 adduced. This Validation Report is not an endorsement of Cisco Catalyst Switches 3k by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and verdicts of the ETR. The validation team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). The evaluation also showed that the product met all the security requirements and Assurance Activities contain in a Protection Profile. 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 Final Evaluation Technical Report for Cisco Catalyst Switches 3k ETR parts 1 and 2 and the associated test report produced by Leidos.

1.2 Evaluation Details

Item	Identifier
Evaluated Product	Cisco Catalyst Switches (3560C, 3560X, and 3750X)
Sponsor & Developer	Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	January 2014
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009
PP	U.S. Government Security Requirements for Network Devices (pp_nd_v1.0) version 1.0, 10 December 2010
Evaluation Class	Evaluation Assurance Level (EAL) 1 consistent with NDPP Assurance Requirements
Disclaimer	The information contained in this Validation Report is not an endorsement of the Cisco Catalyst Switches 3k by any agency of the U.S. Government and no warranty of Cisco Catalyst Switches 3k is either expressed or implied.
Evaluation Personnel	Tony Apted M. Evencie Pierre Kevin Steiner Khai Van
Validation Personnel	Paul Bicknell Brad O'Neill

1.3 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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

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 Validated Products List.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title	Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4 Security Target, Revision 1.0, January 16, 2014
TOE Identification	Cisco Catalyst Switches (3560C, 3560X, and 3750X)
TOE Hardware	Cisco Catalyst Switches 3560C, 3560X, and 3750X)
TOE Software	Cisco IOS 15.0(2)SE4

1.4 TOE Threats, Assumptions, and Organizational Security Policies

All Threats to the TOE, Assumptions, and Organization Security Polices are consistent with those contained in: [NDPPv1.0].

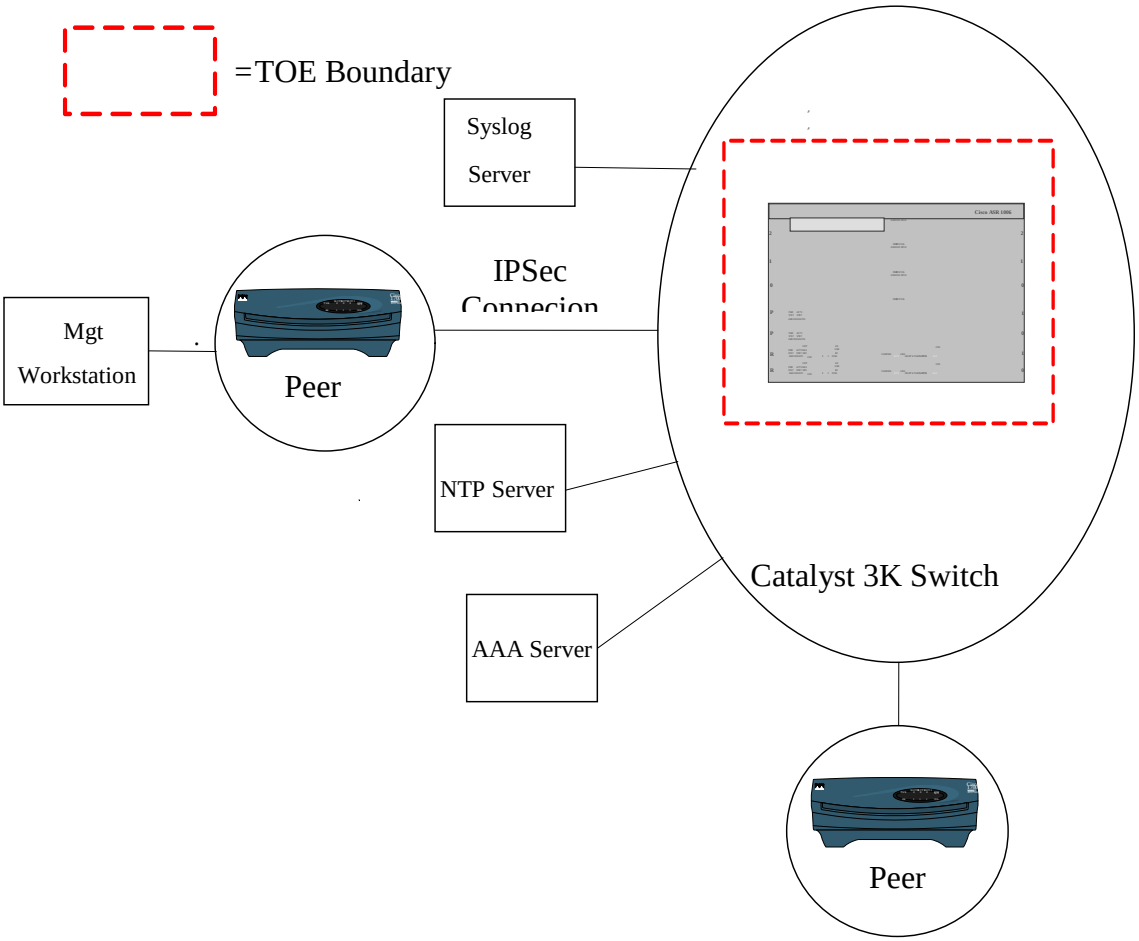
1.5 Architectural Information

The TOE consists of one or more physical devices; the Catalyst Switch with Cisco IOS software. All of the Catalyst Switches run the same version of the IOS 15.0(2)SE4 (FIPS Validated) software which enforces the security functions being claimed regardless of the model. The Catalyst Switch has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS configuration determines how packets are handled to and from the switches' network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination. BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2, Routing protocols are used on all of the Catalyst Switch models.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the Catalyst Switch is to be remotely administered, then the management station must be connected to an internal network, a secure IPsec tunnel must be used to connect to the switch. A syslog server can also be used to store audit records. A remote authentication server can also be used for centralized authentication. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

The following figure provides a visual depiction of an example TOE deployment.

Figure 1: TOE Deployment Example



1.6 Physical Boundaries

The Target of Evaluation includes the following components:

- Cisco Catalyst 3560C Switches

- Cisco Catalyst 3560X Switches
- Cisco Catalyst 3750X Switches
- All Switches run IOS 15.0.(2)SE4
- TOE Guidance

1.7 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 documentation for the TOE is:

- Cisco Catalyst 3560C, 3560X and 3750X Switches Common Criteria User Guidance and Preparative Procedures, version 5.8, 30 January 2014
- Cisco IOS Command Reference
- Cisco IOS Configuration Fundamentals
- Cisco IOS Configuration Guide

The security target used is:

- Cisco Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4 Security Target, version 1.0, January 16, 2014

1.8 Security Policy

Security audit

The TOE generates a comprehensive set of audit logs that identify specific TOE operations. Auditable events include; modifications to the group of users that are part of the authorized administrator roles, all use of the user identification mechanism, any use of the authentication mechanism, any change in the configuration of the TOE, any matching of packets to access control entries in ACLs when traversing the TOE; and any failure of a packet to match an access control list (ACL) rule allowing traversal of the TOE.

The TOE is configured to store the audit logs on an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure.

Cryptographic support

The TOE provides cryptography support for secure communications and protection of information when configured in FIPS mode. The crypto module is FIPS 140-2 SL2 validated (certificate number 1940). The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; digital signature using RSA; cryptographic hashing using SHA1; keyed-hash message authentication using HMAC-SHA1, and IPsec for authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE also implements IPsec secure protocol for secure remote administration. In the evaluated configuration, the TOE must be operated in FIPS mode of operation per the FIPS Security Policy (certificate 1940).

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 for padding so that residual data from previous traffic is never transmitted from the TOE.

Identification and authentication

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user and privileged command modes. 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. Only after the administrative user presents the correct identification and authentication credentials will access to the TOE functionality be granted.

The TOE can be configured to display an advisory banner when administrators log in and also to terminate administrator sessions after a configured period of inactivity.

The TOE also supports authentication of other routers using router authentication supported by BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. Each of these protocols supports authentication by transmission of MD5-hashed password strings, which each neighbor router uses to authenticate others. It is noted that per the FIPS Security Policy, that MD5 is not a validated algorithm during FIPS mode of operation. For additional security, it is recommended router protocol traffic also be isolated to separate VLANs.

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 via IPsec, a terminal server directly connected to the Catalysis Switch (RJ45), or a local console connection (serial port). The TOE provides the ability to perform the following actions:

- allows authorized administrators to add new administrators,
- start-up and shutdown the device,
- create, modify, or delete configuration items,
- create, modify, or delete information flow policies,
- create, modify, or delete routing tables,
- modify and set session inactivity thresholds,

- modify and set the time and date,
- and create, delete, empty, and review the audit trail

All of these management functions are restricted to the authorized administrator of the TOE. The TOE switch platform maintains administrative privilege level and non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. The administrative privilege levels include:

- Administrators are assigned to privilege levels 0 and 1. Privilege levels 0 and 1 are defined by default and are customizable. These levels have a very limited scope and access to CLI commands that include basic functions such as login, show running system information, turn on/off privileged commands, logout.
- Semi-privileged administrators equate to any privilege level that has a subset of the privileges assigned to level 15; levels 2-14. These levels are undefined by default and are customizable.
- Privileged administrators are equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and access controls to limit configuration to authorized administrators. The TOE provides secure transmission when TSF data is transmitted between the TOE and other IT entities, such as remote administration and secure transmission of the audit logs via IPsec. The TOE is also able to detect replay of information and/or operations. The detection applied to network packets that are terminated at the TOE, such as trusted communications between the administrators to TOE, IT entity (e.g., authentication server) to TOE. If replay is detected, the packets are discarded.

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. Alternatively, an NTP server can be used to synchronize the date-timestamp. Finally, the TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module.

Resource utilization

The TOE provides the capability of controlling and managing resources so that a denial of service will not occur. The resource allocations are configured to limit the number of concurrent administrator sessions.

TOE Access

The TOE can terminate inactive sessions after an authorized administrator configurable time- period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

The TOE also provides the administrator with the ability to display a notification of use

banner on the CLI management interface prior to allowing any administrative access to the TOE.

Trusted Path/Channels

The TOE establishes a trusted path between the appliance and the CLI, syslog server, NTP server and if configured, an external authentication server using IPsec.

1.9 Independent Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an NDPPv1.0 EAL1 evaluation.

Independent testing took place at the CCTL location in Columbia, Maryland from March 2013 and again in January 2014.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE (in three distinct but representative configurations) in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory.

This effort involved installing and configuring the Cisco Catalyst Switches 3k components in their respective tiers on a representative subset of the supported operating systems. Subsequently, the evaluators exercised all the tests cases. The tests were selected in order to ensure that each of the test assertions defined by the NDPPv1.0 was covered.

Also, the evaluators devised independent tests to ensure that start-up and shutdown operations were audited, to verify the claimed methods of audit storage, to verify that administrator actions were audited, to verify that users are identified and authenticated, to verify use and restrictions of the management functions, to verify protected communication between the TOE and the trusted components of the operational environment, to verify trusted path and to verify protected update of the TOE software.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for NDPPv1.0 are fulfilled.

1.10 Evaluated Configuration

The TOE is Cisco Catalyst Switches 3k installed and configured according to the Cisco Cat 3k Common Criteria Preparative and Operational Guide as well as the Installation Guide for the respective Cisco Catalyst Switches models included in the TOE.

1.11 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, the NDPPv1.0 and the CCEVS.

The results of the assurance requirements are summarized in this section. The details of the evaluation results are recorded in the Evaluation Technical Report (proprietary) and Test Summary Report provided by the CCTL. 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 version 3.1 R3 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Network Devices Protection Profile (NDPP). The evaluation determined the Cisco Catalyst Switches 3k TOE to be Part 2 extended, and meets the SARs contained the PP.

Below lists the assurance requirements the TOE was required to be evaluated at Evaluation Assurance Level 1. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative user guidance
- ALC_CMC.1 Labeling of the TOE
- ALC_CMS.1 TOE CM coverage
- 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_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability analysis

1.12 Validator Comments/Recommendations

The validators note that the TOE utilizes a non-FIPS approved algorithm (MD5) in the meeting of the Trusted Update SFR (i.e., FPT_TUD_EXT.1.3) that does not meet the intent of the ND PP as expressed in an Application note. However, NIAP management has decided to accept this implementation for this evaluation and plans to clarify the intent of the SFR in future versions of the ND PP. The validators also note that the vendor has indicated that future version of the product will not be relying on MD5 to meet the SFR.

1.13 Annexes

Not applicable.

1.14 Security Target

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

1.15 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

1.16 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 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

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

[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 Catalyst Switches (3560C, 3560X, and 3750X) Running IOS 15.0(2)SE4, parts 1 and 2 (and associated AAR and test report), version 1.0, August 2013.