Certification Report

Cisco Integrated Services Routers (ISR) 4000 Family v3.13.2

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 03 September 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Cisco Integrated Services Routers (ISR) 4000 Family v3.13.2 (hereafter referred to as Cisco ISR v3.13.2), from Cisco Systems, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Cisco ISR v3.13.2 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 and the VPN Gateway Extended Package v1.1 (hereafter referred to as the NDPP).

Cisco ISR v3.13.2 is a routing platform that provides connectivity and security services onto a single, secure device for mid-range enterprise space customers. The TOE, in support of the routing capabilities, provides IPsec connection capabilities for VPN enabled clients connecting through the TOE.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 03 September 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Cisco ISR v3.13.2, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the Cisco ISR v3.13.2 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1   Identification of Target of Evaluation

Cisco Integrated Services Routers (ISR) 4000 Family v3.13.2 (hereafter referred to as Cisco ISR v3.13.2), from Cisco Systems, Inc., is the Target of Evaluation. The Cisco ISR v3.13.2 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

2   TOE Description

Cisco ISR v3.13.2 is a routing platform that provides connectivity and security services onto a single, secure device for mid-range enterprise space customers. The TOE, In support of the routing capabilities, provides IPsec connection capabilities for VPN enabled clients connecting through the TOE.

A diagram of the Cisco ISR v3.13.2 architecture is as follows;
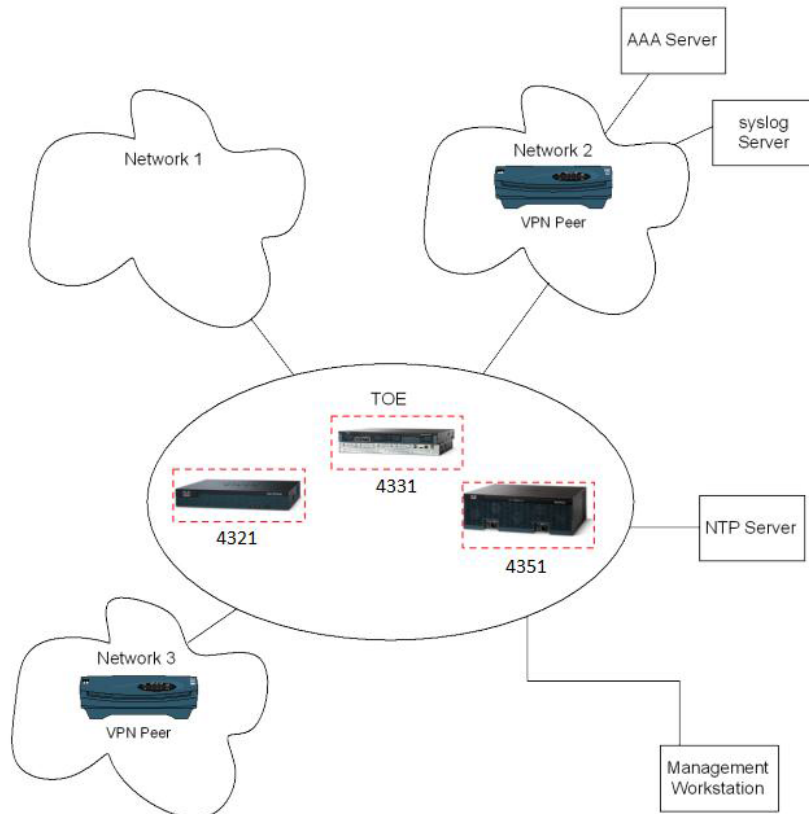
3   Security Policy

Cisco ISR v3.13.2 implements a role-based access control policy to control administrative access to the system. In addition, Cisco ISR v3.13.2 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Residual Information Protection
- Identification and Authentication
- Security Management
- Packet Filtering
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	Certificate
IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5)	*#2388*

4   Security Target

The ST associated with this Certification Report is identified below:

Security Target for Cisco Integrated Services Routers (ISR) 4000 Family v1.0, 10 December 2015

5   Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

Cisco ISR v3.13.2 is:

a. Conformant to the Protection Profile for Network Devices, v1.1, 8 June, with Errata #2 and the Network Device Protection Profile Extended Package VPN Gateway, Version 1.1, 12 April 2013

b. Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

- FAU_STG_EXT.1 - External audit trail storage
- FCS_CKM_EXT.4 - Cryptographic key zeroization
- FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
- FCS_HTTPS_EXT.1 - HTTPS
- FCS_TLS_EXT.1 - TLS
- FIA_PMG_EXT.1 - Password management
- FIA_UIA_EXT.1 - User identification and authentication
- FIA_UAU_EXT.2 - Password-based authentication mechanism
- FPT_SKP_EXT.1 - Protection of TSF data
- FPT_APW_EXT.1 - Protection of administrator passwords
- FPT_TUD_EXT.1 - Trusted update
- FPT_TST_EXT.1 - TSF testing
- FTA_SSL_EXT.1 - TSF-initiated session locking
- FCS_IPSEC_EXT.1 - Internet Protocol Security (IPsec) Communications
- FPF_RUL_EXT.1 - Packet Filtering
- FIA_X509_EXT.1 - X.509 Certificates
- FCS_SSH_EXT.1 - Explicit: SSH
- FIA_PSK_EXT.1 - Pre-Shared Key Composition

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6   Assumptions and Clarification of Scope

Consumers of Cisco ISR v3.13.2 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1   Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- 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; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

6.2   Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3   Clarification of Scope

Cisco ISR v3.13.2 incorporates a CMVP validated cryptographic module that is being claimed as "Vendor Affirmed" in accordance with FIPS IG G.5.

The scope of the evaluation is limited to secure management of the TOE and the VPN gateway functions.

7   Evaluated Configuration

The evaluated configuration for Cisco ISR v3.13.2 comprises:

The TOE firmware (v3.13.2) running on the evaluated TOE hardware (ISR models 4321, 4331, 4351) configured with a VPN peer or endpoint with the following in the environment;

- GPC as a Management Workstation
- NTP Server
- Syslog Server

The publication entitled Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) CC Configuration Guide, v1.0, 12 November 2015 describes the procedures necessary to install and operate Cisco ISR v3.13.2 in its evaluated configuration.

8   Documentation

The Cisco Systems, Inc. documents provided to the consumer are as follows:

a. Cisco 4000 Series ISRs Software Configuration Guide, OL-29328-03, 08 January 2015

b. Troubleshooting Guide for the Cisco 4451-X Integrated Services Router, OL-29313-01

c. Cisco 4000 Series Integrated Services Routers Release Notes, OL-29478-05, 02 February 2015; and

d. Security Target for Cisco Integrated Services Routers (ISR) 4000 Family v1.0, 12 November 2015.

9   Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Cisco ISR v3.13.2, including the following areas:

Development: The evaluators analyzed the Cisco ISR v3.13.2 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the Cisco ISR v3.13.2 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the Cisco ISR v3.13.2 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Cisco ISR v3.13.2 configuration management system and associated documentation was performed. The evaluators found that the Cisco ISR v3.13.2 configuration items were clearly marked.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP and the VPN gateway extended package to which the TOE is claiming conformance.

10.2 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.3 Conduct of Testing

Cisco ISR v3.13.2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evalution and Test Facility. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.4 Testing Results

The independent tests yielded the expected results, providing assurance that Cisco ISR v3.13.2 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
EP	Extended Package
ETR	Evaluation Technical Report
GW	Gateway
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
NDPP	Protection Profile for Network Devices
NTP	Network Time Protocol
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network

13 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Protection Profile for Network Devices, v1.1, June 8, 2012.

e. Security Target for Cisco Integrated Services Routers (ISR) 4000 Family v1.0, 10 December 2015

f. Cisco Integrated Services Routers (ISR) 4000 Family (4321, 4331 and 4351) Common Criteria NDPP Evaluation Technical Report (ETR) v0.7, 3 September 2015.