National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco Systems, Inc, 170 West Tasman Dr., San Jose, CA 95134

Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR)

Report Number:	**CCEVS-VR-10425-2011**
Dated:	**11 July 2011**
Version:	**0.1**

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

Jandria Alexander
Aerospace Corporation
Columbia, MD

Michelle Brinkmeyer
National Security Agency
Fort Meade, MD

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Gary Grainger
Quang Trinh
Science Applications International Corporation
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 Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) solution provided by Cisco Systems, Inc. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Science Applications International Corporation (SAIC) Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in July 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) TOE is a purpose-built, routing platform that includes firewall and VPN functionality. The firewall functionality included within the TOE provides the functionality specified in the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The TOE includes fourteen (14) hardware models, Cisco 881 ISR, Cisco 881G ISR, Cisco 891 ISR, Cisco 1905 ISR, Cisco 1921 ISR, Cisco 1941 ISR, Cisco 2901 ISR, Cisco 2911 ISR, Cisco 2921 ISR, Cisco 2951 ISR, Cisco 3925 ISR, Cisco 3925E ISR, Cisco 3945 ISR, and Cisco 3945E ISR.

The Target of Evaluation (TOE) 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). This Validation Report applies only to the specific version of the TOE as evaluated. 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 monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (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.

The SAIC evaluation team concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL 4 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Security Target and analysis performed by the Validation Team.

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) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through 4 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 Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE:	Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) running IOS 15.1.2T3
Protection Profile	U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments, version 1.1, July 25, 2007
ST:	Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Security Target, Version 0.09, June, 2011
Evaluation Technical Report	Evaluation Technical Report For Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) (Proprietary), Version 2.0, July 11, 2011

Item	Identifier
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Jandria Alexander, Aerospace Corporation, McLean, VA Michelle Brinkmeyer, National Security Agency, Fort Meade, MD

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

3.1 TOE Introduction

The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) are router platforms that provide connectivity and security services onto a single, secure device. These routers offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

In support of the routing capabilities, the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) provides IPSec connection capabilities for VPN enabled clients connecting through the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR).

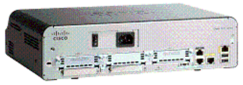
The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) also supports firewall capabilities consistent with the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) are single-device security and routing solutions for protecting the network. The firewall capabilities provided by the TOE are provided implementing security zones. Zone-based firewall allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones facilitates the application of firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface.

3.2 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the following router models Cisco 881 ISR, Cisco 881G ISR, Cisco 891 ISR, Cisco 1905 ISR, Cisco 1921 ISR, Cisco 1941 ISR, Cisco 2901 ISR, Cisco 2911 ISR, Cisco 2921 ISR, Cisco 2951 ISR, Cisco 3925

ISR, Cisco 3925E ISR, Cisco 3945 ISR, and Cisco 3945E ISR. The TOE is comprised of the following:

Hardware	Cisco 881 ISR	Cisco 881G ISR	Cisco 891 ISR	Cisco 1905 ISR	Cisco 1921 ISR
Software	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9
Size	1.75 x 12.8 x 10.4 in.	1.75 x 12.8 x 10.4 in.	1.75 x 12.8 x 10.4 in.	1.73 x 13.5 x 10.8 in.	1.73 x 13.5 x 10.8 in.
Power	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC		
Interfaces	10/100-Mbps Fast Ethernet 4-port 10/100 Mbps managed switch (3) 802.11 b/g antennas	10/100-Mbps Fast Ethernet 4-port 10/100 Mbps managed switch (3) 802.11 b/g antennas	(1) GigE (1) Fast Ethernet 8-port 10/100 Mbps managed switch (3) 802.11 b/g antennas	(1) slots for IT environment provided EHWICs (1) Serial WIC (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (2) 10/100/1000 Port	(2) slots for IT environment provided EHWICs (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (2) 10/100/1000 Port

Hardware	Cisco 1941 ISR	Cisco 2901 ISR	Cisco 2911 ISR	Cisco 2921 ISR	Cisco 2951 ISR
Software	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9
					
Size	1.73 x 13.5 x 10.8 in.	1.72 x 17.5 x 16.5 in.	1.75 x 17.25 x 16.4 in.	3.5 x 17.25 x 16.4 in.	3.5 x 17.25 x 16.4 in.
Power	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
WAN Interfaces	(2) slots for IT environment provided EHWICs (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (2) 10/100/1000 Port	(4) slots for IT environment provided EHWICs (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (2) 10/100/1000 Port	(4) slots for IT environment provided EHWICs (1) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (3) 10/100/1000	(4) slots for IT environment provided EHWICs (1) SFP-based ports (2) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary	(4) slots for IT environment provided EHWICs (1) SFP-based ports (2) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary

			Port	Port (3) 10/100/1000 Port	Port (3) 10/100/1000 Port

Hardware	Cisco 3925 ISR	Cisco 3925E ISR	Cisco 3945 ISR	Cisco 3945E ISR
Software	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9	c880-advipservicesk9
Size	3.5 x 17.1 x 14.7 in.	3.5 x 17.1 x 14.7 in.	5.25 x 17.25 x 16 in.	5.25 x 17.25 x 16 in.
Power	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC	100 to 240 VAC
WAN Interfaces	(4) slots for IT environment provided EHWICs (2) SFP-based ports (2) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (3) 10/100/1000 Port	(3) slots for IT environment provided EHWICs (2) SFP-based ports (2) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (4) GigE Port (4) 10/100/1000 Port	(4) slots for IT environment provided EHWICs (2) SFP-based ports (4) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (3) 10/100/1000 Port	(3) slots for IT environment provided EHWICs (2) SFP-based ports (4) Service module port (1) USB Console Port (1) Serial Console Port (1) Auxilary Port (4) GigE Port (4) 10/100/1000 Port

.

4 Security Policy

This section summaries the security functionality of the TOE:

1. Identification and Authentication
2. Secure Management
3. VPN and/or Firewall Information Flow Control
4. Cryptography
5. Secure Auditing

4.1.1 Identification & Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates itself. Device-level authentication is performed via IKE/IPSec mutual authentication. The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrative interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality.

The TOE optionally facilitates single use authentication for administrative users attempting to connect to the TOE by invoking an external RADIUS AAA (IT environment) to provide single-use authentication. The TOE provides single use authentication to administrative users of the TOE through the use of and external AAA server

4.1.2 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 SSHv2 session via terminal server or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; TOE configuration backup and recovery, and the information flow control policies enforced by the TOE. The TOE supports two separate administrative roles: non-privileged Administrator and privileged Administrator. All of the security relevant management functionality described in the paragraph above can only be performed by the privileged Administrator.

When an administrative session is initially established, the TOE displays an Administrator configurable warning banner. This is used to provide any information deemed necessary by the Administrator. Once a configured threshold of consecutive authentication failures is reached, the TOE locks-out the administrative user attempting to log into the TOE until an administrator unlocks the administrator’s account. An administrative user cannot unlock their account. An administrative user must be unlocked by a different/separate privileged administrative user.

4.1.3 Information Flow Control

The TOE enforces several information flow control policies, including:

- Firewall Information Flow Control
- VPN Information Flow Control
- VLAN Information Flow Control

Each of these enforced information flows are further discussed below.

4.1.3.1 Firewall Information Flow Control

The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) mediate information flows through the TOE for unauthenticated information flows. The TOE provides the ability to classify data flows into zones. Configurable allow or deny rule sets are applied to each information flow on a zone by zone basis. All security attributes are inspected based on the configurable rule set of the information flow. The TOE makes the decision to allow or deny information flows based on the configured information flow rule set.

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.

4.1.3.2 VPN Information Flow Control

Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) deliver VPN connections to remote entities. The VPN process includes remote device authentication, negotiation of specific cryptographic parameters for the session, and providing a secure connection to and from the remote device. For inbound or outbound connections with external IT entities that are capable of supporting VPN (e.g., VPN clients and VPN gateways), the TOE will establish a secure connection. For other inbound or outbound traffic a secure connection will not be established, clear text traffic is explicitly configured in this case.

4.1.3.3 VLAN Information Flow Control

Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) allow VLAN connections to/from remote entities. The TOE provides that ability to identify the VLAN the network traffic is associated with. The TOE then permits or denies the network traffic based on the VLANs configured on the interface the network traffic is received /destined.

4.1.4 Cryptography

The TOE provides cryptography in support of other Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2. The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2. The cryptographic services provided by the TOE include:

Table 2: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPSec session.
Group Domain of Interpretation	Used in IPSec session establishment.
ANSI X9.31 PRNG (3 key TDES-based)	Used in IPSec session establishment.
AES	Used to encrypt IPSec session traffic. Used to encrypt SSHv2 session traffic.

4.1.5 Security Audit

The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) provide extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, information flow control enforcement, identification and authentication, and administrative actions. The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) generate an audit record for each auditable event. The Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) provide the administrator with a sorting and searching capability to improve audit analysis. The administrator configures auditable events, backs-up 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.

5 Assumptions

The following assumptions were made during the evaluation of Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR):

- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
- The TOE does not host public data.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- Information cannot flow among the internal and external networks unless it passes through the TOE.
- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection (e.g., a console port) if the connection is part of the TOE.
- Human users who are not authorized administrators can not access the TOE remotely from the internal or external networks.
- Authorized administrators may access the TOE remotely from the internal and external networks.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR):

6.1 Design Documentation

1. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Security Architecture Specification, Version 0.2, May 6, 2011
2. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Functional Specification, Version 0.54, May 19, 2011
3. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) TOE Design Specification, Version 0. 5, May 6, 2011
4. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Functional Specification Annex B RFC Security Parameter Relevancy, June 2011

6.2 Guidance Documentation

1. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Operational User Guidance and Preparative Procedures, Version 4, July 2011
2. Cisco 860 Series, Cisco 880 Series, and Cisco 890 Series Integrated Services Routers Hardware Installation Guide, Text Part Number: OL-16193-04
3. Cisco 1900 Series Integrated Services Router Hardware Installation, Text Part Number: OL-19084-02
4. Cisco 2900 and 3900 Series Hardware Installation, Text Part Number: OL-18712-01
5. Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers Generation 2, Text Part Number: OL-20697-03
6. Cisco 881, Cisco 881G, Cisco 891 Integrated Services Routers FIPS 140-2 Non-Proprietary Security Policy
7. Cisco 1905 and Cisco 1921 Integrated Services Routers (ISRs) FIPS 140-2 Non-Proprietary Security Policy
8. Cisco 1941, Cisco 2901, Cisco 2911, and Cisco 2921 Integrated Services Routers (ISRs) FIPS 140-2 Non-Proprietary Security Policy
9. Cisco 2951, Cisco 3925, and Cisco 3945 Integrated Services Routers (ISRs) FIPS 140-2 Non-Proprietary Security Policy
10. Cisco 3925E and Cisco 3945E Integrated Services Routers (ISRs) FIPS 140-2 Non-Proprietary Security Policy
11. Cisco IOS Security Command Reference
12. Cisco IOS Configuration Fundamentals Command Reference
13. Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide, Text Part Number: OL-14127-06, February 26, 2010
14. Cisco ASR 1000 Series Aggregation Services Routers Operations and Maintenance Guide, Text Part Number: OL-17665-03, June, 2009
15. Cisco IOS IP Routing: BGP Command Reference, November 2009

16. Cisco IOS IP Routing: ISIS Command Reference, November 2009
17. Cisco IOS IP Routing: OSPF Command Reference, November 2009
18. Cisco IOS IP Routing: RIP Command Reference, November 2009
19. FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20
20. Cisco IOS XE Network Management Configuration Guide, Release 2

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR), August 2011, Version: 1

6.4 Testing

1. Project Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Test Mappings and Introduction, Version 1.0
2. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan Test Cases Test Bed #1, Revision 2
3. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan Test Cases Using Test Bed #2, Revision 2
4. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan Test Cases Using Test Bed #3, Revision 2
5. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan test Cases Using Test Bed #4, Revision 2
6. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan Test Cases GETVPN Test Bed, Revision 2
7. Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Detailed Test Plan Test Cases Test Bed Ixia, Revision 2
8. ISR_Common_Criteria_Test_Coverage_and_Depth-06032011.xls, 6/3/2011

7 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Evaluation Team Test Report for the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR), Version 2.0, July 11, 2011.

7.1 Developer Testing

At EAL4, testing must demonstrate correspondence between the tests and the functional specification. The vendor testing addressed each of the security functions identified in the ST and interfaces in the design. These security functions include:

1. Identification and Authentication
2. Secure Management
3. VPN and/or Firewall Information Flow Control
4. Cryptography
5. Secure Auditing

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the Common Criteria Guide, ran a sample of the developer tests and verified the results, then developed and performed functional and vulnerability testing that augmented the vendor testing by exercising different aspects of the security functionality.

The evaluation team testing focused on testing boundary conditions not tested by Cisco. The evaluation team tested combinations of the information flow policies that Cisco did not test. For vulnerability testing the evaluation team performed port and vulnerability scanning as well as other team developed tests.

8 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) including:

- fourteen (14) hardware models, Cisco 881 ISR, Cisco 881G ISR, Cisco 891 ISR, Cisco 1905 ISR, Cisco 1921 ISR, Cisco 1941 ISR, Cisco 2901 ISR, Cisco 2911 ISR, Cisco 2921 ISR, Cisco 2951 ISR, Cisco 3925 ISR, Cisco 3925E ISR, Cisco 3945 ISR, and Cisco 3945E ISR
- all models running IOS 15.1.2T3

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Common Criteria Operational User Guidance and Preparative Procedures** document.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all EAL2 augmented with ALC_FLR.2 work units received a passing verdict.

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 CC version 3.1 rev 3 and CEM version 3.1 rev 3. The evaluation determined the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 4) augmented with ALC_FLR.2 requirements.

The following evaluation results are extracted from the non-proprietary Evaluation Technical Report provided by the CCTL, and are augmented with the validator's observations thereof.

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 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) 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 EAL 4 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 and a detailed design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

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 EAL 4 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. Both of these 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 EAL 4 ALC CEM work unit. The evaluation team ensured the adequacy of the developer procedures to protect the TOE and the TOE documentation during TOE development and maintenance to reduce the risk of the introduction of TOE exploitable vulnerabilities during TOE development and maintenance. The ALC evaluation also ensured the TOE is identified such that the consumer is able to identify the evaluated TOE. The evaluation team ensured the adequacy of the procedures used by the developer to accept, control and track changes made to the TOE implementation, design documentation, test documentation, user and administrator guidance, security flaws and the CM documentation.

In addition to the EAL 4 ALC CEM work units, the evaluation team applied the ALC_FLR.2 work units from the CEM supplement. The flaw remediation procedures were evaluated to ensure that flaw reporting procedures exist for managing flaws discovered in the TOE.

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 EAL 4 ATE CEM work unit. The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the vendor test documentation sufficiently addresses the security functions as described in the functional specification. The evaluation team re-ran the entire vendor test suite, and devised an independent set of team test and penetration tests. The vendor tests, team tests, and penetration tests substantiated the security functional requirements in the ST.

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 EAL 4 AVA CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon the developer strength of function analysis, the developer vulnerability analysis, the evaluation team’s vulnerability analysis, and the evaluation team’s performance of penetration tests.

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 performance of the entire vendor tests suite, the independent tests, and the penetration test 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 validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

The evaluation team observed that the vendor's security tests are predominantly manual and apparently not closely integrated with the extensive automated testing performed as a routine part of product development. While these evaluated tests are sufficient to satisfy Common Criteria requirements, the validation team recommends a closer integration in future efforts, in order to improve test integration and provide greater test coverage.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as *Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Security Target, Version 0.09, June 2011*.

13 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 to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **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.

14 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] Science Applications International Corporation. *Evaluation Technical Report for the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Part 2 (Proprietary)*, Version 2.0, July 11, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR), ETR Part 2 Supplement (SAIC and Cisco Proprietary),* Version 2.0, July 11, 2011.

Note: This document was used only to develop summary information regarding the testing performed by the CCTL.

[10] Cisco 800, 1900, 2900, 3900 Series Integrated Service Routers (ISR) Security Target, Version 0.09, June 2011.