National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco 5915 Embedded Services Router

Report Number: CCEVS-VR-VID10493-2013
Dated: 29 April 2013
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

Validation Team

Mike Allen (Lead Validator)
Jandria S. Alexander (Senior Validator)
Aerospace Corporation
Columbia, Maryland

Common Criteria Testing Laboratory

Gary Grainger
James Arnold
Tammy Compton
Julie Cowan
Chris Keenan
Science Applications International Corporation
Columbia, Maryland

Table of Contents

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification Agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10 where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco 5915 Embedded Services Router. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This Validation Report applies only to the specific version and configuration of the product as evaluated and documented in the Security Target.

The evaluation of the Cisco 5915 Embedded Services Router 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 September 2012.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Report (ETR) and associated test report. The ST was written by Cisco Systems, Inc. The ETR and test report used in developing this validation report were written by SAIC. The evaluation was performed to conform to the requirements of the Common Criteria for Information Technology Security Evaluation, Version 3.1 R3, dated July 2009 at Evaluation Assurance Level 2 (EAL 2) augmented with ALC_FLR.2 and ALC_DVS.1 and the Common Evaluation Methodology for IT Security Evaluation (CEM), Version 3.1 R3, dated July 2009. The product, when configured as specified in the installation guides, user guides, and Security Target satisfies all of the security functional requirements stated in the Cisco 5915 Embedded Services Router Security Target. The evaluation team determined the product to be both Part 2 extended and Part 3 augmented compliant, and meets the assurance requirements of EAL 2 augmented by ALC_FLR.3 and ALC_DVS.1. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is the Cisco 5915 ESR (conduction-cooled or air-cooled models) running IOS 15.2(2)GC. The TOE is a ruggedized router designed for use in harsh environments offering reliable operation in extreme temperatures and under shock and vibration conditions typical for mobile applications in rugged terrain.

The validation team monitored the activities of the evaluation team, 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 2 augmented with ALC_FLR.2 and ALC_DVS.1) have been met.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, 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 conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology (IT) 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 (if any); and
- 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
Target of Evaluation	Cisco 5915 Embedded Services Router running IOS 15.2(2)GC
Protection Profiles	None.
Security Target	*Cisco 5915 Embedded Services Router Security Target*, Revision 0.10, 13 September, 2012
Dates of evaluation	January 2012 through September 2012
Evaluation Technical Report	*Evaluation Technical Report for the Cisco 5915 Embedded Services Router Part 1 (Non-Proprietary)*, Version 1.0, July 31, 2012 *Evaluation Technical Report for the Cisco 5915 Embedded Services Router (Proprietary)*, Version 2.0, July 31, 2012
Conformance Result	Part 2 extended conformant and EAL2 Part 3 augmented with ALC_FLR.2 and ALC_DVS.1
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on January 19, 2012
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July2009 and all applicable NIAP and International Interpretations effective on November 8, 2011
Sponsor	Cisco Inc., 170 West Tasman Drive, San Jose, CA 95134
Developer	Cisco Inc.
Common Criteria Testing Lab	SAIC Inc., Columbia, MD
Evaluators	Greg Beaver, Jonathan Alexander and Rory Saunders
Validation Team	Jandria S. Alexander and Mike Allen of the Aerospace Corporation

3 Security Policy

This section summaries the security functionality of the TOE:

1. Security audit
2. Cryptographic support
3. User data protection
4. Identification and authentication
5. Secure Management
6. Protection of the TSF
7. TOE access
8. Intrusion Prevention Services

3.1 Security Audit

The TOE generates audit messages that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: 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 will write audit records to the local logging buffer by default and can be configured to send audit data via syslog to a remote audit server, or display to the CLI console. These audit messages include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment.

3.2 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 SL1 validated, certificate number 1935. 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 SSHv2 for secure remote administration. For GDOI, the TOE can perform the role of the GDOI key server and the group controller.

3.3 Traffic Filtering and Switching (ACLs)

This product supports IP ACLS, VPN policies and VLANs.

IP ACLs control whether routed IP packets are forwarded or blocked at the TOE interfaces that have been configured with IP addresses. The TOE examines each frame and packet to determine whether to forward or drop it, on the basis of criteria specified within the access lists applied to the interfaces through which the traffic would enter and leave the TOE. For those interfaces configured with Layer-3 addressing the ACLs can be configured to filter IP traffic using: the source address of the traffic; the destination address of the traffic; and the layer 3 and 4 protocol

identifier. Use of Access Control Lists (ACLs) also allows restriction of remote administration connectivity to specific interfaces of the TOE so that sessions will only be accepted from approved management station addresses identified as specified by the administrator.

Cisco 5915 ESR delivers 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., a VPN Peer), the TOE will establish a secure connection. For other inbound or outbound traffic a secure connection will not be established.

Cisco 5915 ESR allows VLAN connections to/from remote entities. The TOE provides the 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. This policy is applied after the Firewall policy.

3.4 Identification and Authentication

The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC 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 (via EXEC mode), 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 supports use of a remote AAA server (RADIUS and TACACS+) as the enforcement point for identifying and authenticating users, including login and password dialog, challenge and response, and messaging support. Encryption of the packet body is provided through the use of RADIUS (note RADIUS only encrypts the password within the packet body, while TACACS+ encrypts the entire packet body except the header).

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 performs device-level authentication of the remote device (VPN peers). 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 v1/IPSec v3 mutual authentication.

3.5 Security Management

The TOE allows authorized administrators to add new administrators, start-up and shutdown the device, create, modify, or delete configuration details such as interface parameters and ACLs, and to modify and set the time and date. All TOE administration occurs either through a secure SSH session via a SSH client, or via a local console connection.

The TOE router platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS privilege level 15 (has all privileges on the box); and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. The term "authorized administrator" is used in this ST to refer to any user which has been assigned to a privilege level is permitted to perform the relevant action; therefore has the appropriate privileges to perform the requested functions.

The TOE also supports external IT entities. These external IT entities are peer routers that pass network control information (e.g., routing tables) to the TOE. Also included are any other VPN peers with whom the TOE exchanges information, including VPN clients and VPN gateways.

3.6 Protection of the TSF

The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)). 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 timestamp that is applied to TOE generated audit records. Alternatively, an NTP server can be used to synchronize the clock.

Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

3.7 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 can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

3.8 Intrusion Prevention Services

The Cisco 5915 ESR IOS software Intrusion Prevention System (IPS) operates as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When Cisco IOS IPS

detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages stored in the local buffer and then offloaded to an external syslog server. The privileged administrator can configure Cisco IOS IPS to choose the appropriate response to various threats. When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an audit record to a syslog server or a management interface
- Drop the packet
- Reset the connection
- Deny traffic from the source IP address of the attacker for a specified amount of time
- Deny traffic on the connection for which the signature was seen for a specified amount of time

For inbound packets the IDS processing is done after IP ACLs and then VPN policies have been applied.

4 Assumptions and Clarification of Scope

The assumptions, threats and policies in the following paragraphs were considered during the evaluation of the Cisco 5915 Embedded Services Router.

4.1 Assumptions

The following assumptions were made during the evaluation of Cisco 5915 ESR:

- The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance; however, they are capable of error.
- Administrators will be trained to periodically review audit logs to identify sources of concern
- Personnel will be trained in the appropriate use of the TOE to ensure security.
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
- Copies of TOE configuration data including representations of authentication data maintained off the TOE in hard-copy or soft-copy will be kept confidential and access will be limited to authorized administrators. Audit data transmitted by the TOE and routing table updates exchanged with neighbor routers, and associated neighbor router authentication data will be protected from unauthorized disclosure through isolation of associated network traffic.
- The TOE will be able to function with the software and hardware of other router vendors on the network.
- The threat of malicious attacks aimed at exploiting the TOE is considered low.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation and how the TOE needs to be configured to ensure it operates in the evaluated configuration.

The following functionality included as part of the product was excluded from the evaluation and should not be used when the product is in the evaluated configuration:

- Non-FIPS 140-2 mode of operation on the router. This mode of operation includes non-FIPS allowed operations.

In addition, Cisco IOS contains a collection of features that build on the core components of the system. These features are enabled by default and must be disabled in the evaluated configuration:

- Telnet: Sends authentication data in plain text. This feature is enabled by default and must be disabled in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.

The following features are disabled by default and must remain disabled in the evaluated configuration:

- SNMP does not enforce the required role privileges. This feature is disabled by default and cannot be configured for use in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target.
- HTTP Server for web user interface management: Sends authentication data in plain text and does not enforce the required role privileges. Not including this feature does not interfere with the management of TOE as defined in the Security Target.
- IEEE 802.11 Wireless Standards: The evaluated configuration of 5915 Routers as described is this Security Target does not support implementing wireless local area network. Use of this feature requires additional hardware beyond what is included in the evaluated configuration.
- MAC address filtering: The SFPs in the Security Target are defined as information flow polices, not access polices that allow access based on MAC address
- Flexible NetFlow: Used for a traffic analysis and optimization, and SFRs do not include performance/optimization features. Not including this feature does not interfere with the enforcement of the security policies as defined in the Security Target.
- The Network Assistant application and CiscoWorks LAN Management Solutions are separate licensed, separate products and are not included in the scope of this evaluation.

Apart from these exceptions all types of network traffic through and to the TOE are within the scope of the evaluation.

5 Architectural Information

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

The Cisco 5915 ESR is a router platform used to construct IP networks by interconnecting multiple smaller networks or network segments. The TOE provides connectivity and security services onto a single, secure device. The flexible, compact form factor of these routers, complemented by Cisco IOS® Software, provides highly secure data, voice, and video communications to stationary and mobile network nodes across wired links.

In support of the routing capabilities, the 5915 ESR provides IPSec connection capabilities for VPN enabled clients connecting through the 5915 ESR. The 5915 ESR is also compatible with VPN clients that use GDOI.

The 5915 ESR is a PCI-104 router module solution for protecting the network. The firewall capabilities provided by the TOE are provided via a stateful packet filtering firewall. A stateful packet filtering firewall controls the flow of IP traffic by matching information contained in the headers of connection-oriented or connection-less IP packets against a set of rules specified by the authorized administrator for firewalls. This header information includes source and destination host (IP) addresses, source and destination port numbers, and the transport service application protocol (TSAP) held within the data field of the IP packet. Depending upon the rule and the results of the match, the firewall either passes or drops the packet. The stateful firewall remembers the state of the connection from information gleaned from prior packets flowing on the connection and uses it to regulate current packets. The packet will be denied if the security policy is violated.

In addition to IP header information, the TOE mediates information flows on the basis of other information, such as the direction (incoming or outgoing) of the packet on any given firewall network interface. For connection-oriented transport services, the firewall either permits connections and subsequent packets for the connection or denies the connection and subsequent packets associated with the connection.

The TOE also includes on the 5915 Embedded Services Router modules a network-based Intrusion Prevention System that monitors traffic in real-time. It can analyze both the header and content of each packet. The TOE uses a rule-based expert system to interrogate the packet information to determine the type of attack, be it simple or complex.

5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 2: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Chassis	Yes	The router supports Input/Ouput connectors through standard

Component	Required	Usage/Purpose Description for TOE performance
		RJ-45 connectors, or any other cPCI compatible network connector. The chassis can be any off-the-shelf module that is capable of holding a PCI-104 form factor.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Authentication Server	No	The authentication server (RADIUS and TACACS+) is used to provide centralized authentication and related auditing for one or more distributed instances of the TOE.
VPN Peer	No	This includes any peer with which the TOE participates in VPN communications. VPN peers may be any device or software client that supports IPSec v3 communications. Both VPN clients and VPN gateways are considered VPN peers by the TOE.
NTP Server	No	The TOE supports communications with an NTP server. A solution must be used that supports MD5 hashing of communications with up to a 32 character key.
Syslog Server	No	The syslog audit server is used for remote storage of audit records that have been generated by and transmitted from the TOE.

5.2 TOE DESCRIPTION

This section provides an overview of the 5915 ESR Target of Evaluation (TOE). The TOE is comprised of a single PCI-104 router module running IOS 15.2(2)GC.

5.3 TOE Evaluated Configuration

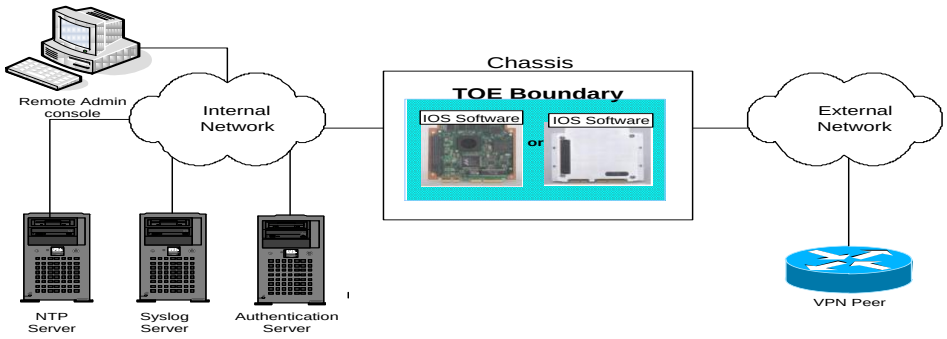
Table 1: Evaluated Configurations

TOE	• One or more Cisco 5915 Embedded Security Routers (conduction-cooled or air-cooled models) • Each router running IOS 15.2(2)GC (FIPS validated)

The TOE can optionally connect to an NTP server on its internal network for time services. A syslog server can also be used to store audit records. 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.

If the TOE is to be remotely administered, SSHv2 must be used for that purpose. All administrative capabilities can be performed either remotely via SSHv2 or locally using the console port. Both methods access the same Command Line Interface (CLI) functionality.

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



5.4 Physical Scope of the TOE

The TOE is a hardware solution obtained from HCL under OEM contract running the IOS 15.2(2)GC software solution. The image name for the 5915 ESR TOE is c5915-adventerprisek9-mz.SPA.152-1.GC1.bin.

The key components on the board are:

- Freescale MPC8358E processor
- Marvell 88E6046 six port Ethernet switch (only 3 ports are used)
- Broadcom BCM5221 Ethernet PHY
- Numonyx PC28F00BM29EWH NOR flash chip

Both an air-cooled and a conduction-cooled board exist. They differ only in cooling mechanism. The very same circuit board/components are used, but the conduction cooled version includes thermal plates.

The board provides the following external interfaces:

- RS-232 Console port accessible via card edge fingers
- (2) Routed FE ports, (3) Switched FE ports
- JTAG: A JTAG chain is present on the board (connects to the uP and a CPLD). The JTAG interface connects to the card edge fingers. It is to be disabled in the evaluated configuration and not re-enabled

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco 5915 ESR:

6.1 Design Documentation

1. Cisco 5915 Embedded Services Router Security Architecture Document Draft, Revision 0.2, May 23, 2012
2. Cisco 5915 Embedded Services Router Functional Specification, Revision 0.2, May 23, 2012
3. Cisco 5915 Embedded Services Router TOE Design Specification, Revision 0.2, May 23, 2012
4. Annex A: Security Relevant CLI Commands, March 16, 2012
5. Annex B: RFC Security Parameter Relevancy, May 23, 2012

6.2 Guidance Documentation

Title	Link
Release Notes for Cisco IOS Release 15.2(2)GC, May 29, 2012	http://www.cisco.com/en/US/products/ps10148/prod_release_notes_list.html
Cisco 5915 Embedded Services Router Hardware Technical Reference Guide, Last Updated: April 2012	http://www.cisco.com/en/US/docs/solutions/GGSG-Engineering/Cisco_5915/Hardware_Install_Guide/5915hw.html
Configuration Fundamentals Configuration Guide Cisco IOS Release 15.2MT	https://www.cisco.com/en/US/docs/ios-xml/ios/fundamentals/configuration/15mt/fundamentals-15-mt-book.html
Securing User Services Configuration Guide Library, Cisco IOS Release 15.2M&T	http://www.cisco.com/en/US/docs/iosxml/ios/security/config_library/15-mt/secuser-15-mt-book.html
Network Management Configuration Guide Library, Cisco IOS Release 15.2M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/net_mgmt/config_library/15-mt/netmgmt-15-mt-library.html
Software Configuration Guide for Cisco IOS Release 15.2(2)GC	http://www.cisco.com/en/US/products/ps10148/products_installation_and_configuration_guides_list.html

Cisco IOS Security Command Reference	http://www.cisco.com/en/US/products/ps11746/prod_command_reference_list.html
Loading and Managing System Images Configuration Guide, Cisco IOS Release 15.2M&T	http://www.cisco.com/en/US/docs/ios-xml/ios/sys-imagemgmt/configuration/15-mt/sysimgmgmt-15-mt-book.html

6.3 Life Cycle

1. Configuration Management, Delivery Procedures, Development Security, and Flaw Remediation for Cisco 5915 Embedded Services Router, June 25, 2012, Version 1.2

6.4 Testing

1. 5915 Common Criteria Detailed Test Plan, Revision 12, 06/01/2012
2. 5915-EAL2-non-NDPP-TestCaseMapping-20120524.xls

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 5915 Embedded Security Router, Version 1.0, July 31, 2012.

7.1 Developer Testing

At EAL2, 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:

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE access
- Intrusion Prevention Services

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according the *Cisco 5915 Embedded Security Router Common Criteria Operational User Guidance and Preparative Procedures*, ran a subset of vendor test suite 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. 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 5915 Embedded Services Router including:

- One or more Cisco 5915 Embedded Security Routers (conduction-cooled or air-cooled models)
- Each router running IOS 15.2(2)GC (FIPS validated)

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco 5915 Embedded Services Router 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 and ALC_DVS.1 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 5915 Embedded Services Router TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 2) augmented with ALC_FLR.2 and ALC_DVS.1 requirements.

10 Validator Comments/Recommendations

The validation team's observations support the evaluation team's conclusion that the Cisco 5915 Embedded Services Router meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

11 Security Target

The Security Target is identified as the Cisco 5915 Embedded Services Router Security Target, Rev 0.10, 13 September 2012. The document identifies the security functional requirements (SFRs) that are levied on the TOE, which are necessary to implement the TOE security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2 augmented with ALC_FLR.3 and ALC_DVS.1.

12 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.

13 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 R3, July 2009.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements, Version 3.1 R3, July 2009.

[3] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements, Version 3.1 R3, July 2009.

[4] Common Criteria Project Sponsoring Organisations. *Common Methodology for Information Technology Security Evaluation*, Version 3.1 R3, July 2009.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 2.0, September 8, 2008.

[6] Science Applications International Corporation. *Evaluation Team Test Report For Cisco 5915 Embedded Services Router, (SAIC and Cisco Proprietary),* Version 2.0, July 31, 2012.

[7] Science Applications International Corporation. *Evaluation Technical Report for the Cisco 5915 Embedded Services Router Part 1 (Non-Proprietary),* Version 1.0, July 31, 2012.

[8] Science Applications International Corporation. *Evaluation Technical Report for the Cisco 5915 Embedded Services Router Part 2 (Proprietary),* Version 2.0, July 31, 2012.

[9] *Cisco 5915 Embedded Services Router Security Target*, Revision 0.10, 13 September 2012.