National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

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

Cisco 5940 Series Embedded Services Router

Report Number: CCEVS-VR-VID10429-2011
Dated: 5 July 2011
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

Jandria Alexander
Aerospace Corporation
Columbia, MD

Ralph Broom
Noblis, Inc.
Falls Church, VA

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
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 5940 Series Embedded Services Router 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 June 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 2 augmented with ALC_FLR.2.

The Cisco 5940 Series Embedded Services Router TOE is a purpose-built, routing platform that includes firewall, Intrusion Prevention, 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 one router module that can operate in any CompactPCI (cPCI) 3 unit (3U) chassis.

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 2 augmented with ALC_FLR.2) have been met.

The technical information included in this report was obtained from the Cisco 5940 Series Embedded Services Router 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 5940 Series Embedded Services Router running IOS 15.1(2)GC1
Protection Profile	U.S. Government Protection Profile for Traffic Filter Firewall For Basic Robustness Environments, version 1.1, July 25, 2007
ST:	Cisco 5940 Series Embedded Services Router Security Target, Version 1.0, June, 2011
Evaluation Technical Report	Evaluation Technical Report For Cisco 5940 Series Embedded Services Router (Proprietary), Version 2.0, June 6, 2011
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 3
Conformance Result	CC Part 2 Extended, CC Part 3 conformant

Item	Identifier
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	SAIC, Columbia, MD
CCEVS Validators	Jandria, Aerospace Corporation, McLean, VA
	Ralph Broom, MITRE Corporation., McLean, VA

3 Architectural Information

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

3.1 TOE Introduction

The Cisco 5940 Series Embedded Services Router is a router platform that 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 Cisco 5940 Series Embedded Services Router provides IPSec connection capabilities for VPN enabled clients connecting through the Cisco 5940 Series Embedded Services Router. The Cisco 5940 Series Embedded Services Router is also compatible with the GET VPN (using GDOI).

The Cisco 5940 Series Embedded Services Router also supports firewall capabilities consistent with the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments. The Cisco 5940 Series Embedded Services Router is a 3U (cPCI) 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 5940 Series 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.

3.2 Physical Scope of the TOE

The TOE is a hardware solution obtained from General Dynamics under OEM contract running the IOS 15.1(2)GC1 software solution. The image name for the 5940 Series Embedded Services Router TOE is c59xx-adventerprisek9-mz.SPA. The key components on the board are:

- Freescale MPC8548E processor
- Marvell 88E1145 quad Ethernet transceiver
- Spansion S29GL01GP flash or Numonyx flash chip

Both an air-cooled and a conduction-cooled board exist. Aside from the differences outlined below, they differ only in cooling mechanism.

The board provides the following external interfaces:

- Serial port.
    - Via a connection on the J2 connector on the cPCI backplane on the conduction-cooled model and via direct access RJ-45 port or the J2 connector on the cPCI backplane on the card on the air-cooled model.
- Four Gigabit Ethernet ports, via connections on the J2 connector on the cPCI backplane.
- PCI interface connection to the backplane. This PCI interface is used to connect to the RTM
- PCI bus connection to the backplane. This PCI controller is disabled within the IOS running on the TOE.

JTAG header. The JTAG will be connected to the J2 connector on the cPCI backplane. It is to be disabled in the evaluated configuration and not re-enabled.

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. Intrusion Prevention Services
5. Cryptography
6. 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 administrators 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 all administrators wishing to connect to the TOEs secure CLI administrative interface. The TOE requires all administrators to authenticate prior to being granted access to any of the management functionality.

The TOE facilitates single-use authentication for all administrators and external IT entities 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 external IT entities through the use of IKE/IPSec mutual authentication.

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 SSH session, via terminal server (such as a Cisco 2811), or via a local console connection. The TOE provides the ability to securely manage all TOE administrators; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE (including settings for an NTP server, if used as the timestamp source); TOE configuration backup and recovery, and the information flow control policies enforced by the TOE. The TOE supports two separate administrative roles that make up the authorized administrator: non-privileged Administrator and privileged Administrator.

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.

Once a configured threshold of consecutive authentication failures is reached, the TOE locks-out the administrator (either privileged or non-privileged) or external IT entity attempting to log into the TOE until another administrator unlocks their account. No administrator can unlock their own account, therefore there should always be at least two privileged administrators configured on the device.

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.

4.1.4 Firewall Information Flow Control

The Cisco 5940 Series Embedded Services Router mediate information flows through the TOE for unauthenticated information flows. The Information Control functionality of the TOE allows privileged administrators to set up rules between interfaces of the TOE. These rules control whether a packet is transferred from one interface to another and/or transferred encrypted based upon:

- Presumed address of source subject
- Presumed address of destination subject
- Service used
- Transport layer protocol
- Network interface on which the connection request occurs and is to depart

Packets will be dropped unless a specific rule or policy in an access control list (ACL) has been set up to allow the packet to pass. The order of Access Control Entries (ACEs) in an ACL is important. When the TOE decides whether to forward or drop a packet, the TOE tests the packet against the ACE in the order in which the entries are listed. After a match is found, no more ACEs are checked such that if the ACE at the beginning of the ACL explicitly permits all traffic, no further ACEs are checked. Interface ACLs are applied first before IPsec negotiations occur in the evaluated configuration.

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

4.1.5 VPN Information Flow Control

Cisco 5940 Series Embedded Services Router 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.

4.1.6 VPN Information Flow Control

Cisco 5940 Series Embedded Services Router 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.

4.1.7 Intrusion Prevention Services

The Cisco 5940 Series Embedded Services Router 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 centralized 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 firewall policies and then VPN policies have been applied.

4.1.8 Cryptography

The TOE provides cryptography in support of other Cisco 5940 Series Embedded Services Router security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 1. Further details regarding the FIPS validation can be found in Certificate #XXXX. The TOE provides cryptography in support of VPN connections and remote administrative management via SSH. 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.
ANSI X9.31 PRNG	Used in IPSec session establishment.
AES	Used to encrypt IPSec session traffic. Used to encrypt SSH session traffic.
Group Domain of Interpretation	Used in IPSec session establishment.
RSA	IKE RSA authentication
DSA	SSH host authentication, SSH client authentication

SHA256	IKE

4.1.9 Security Audit

The Cisco 5940 Series Embedded Services Router provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, information flow control enforcement, intrusion prevention, identification and authentication, and administrative actions. The Cisco 5940 Series Embedded Services Router generates an audit record for each auditable event. These events include a timestamp that can be provided by the TOE or an optional NTP server in the operational environment. The Cisco 5940 Series Embedded Services Router provides the privileged administrator with a sorting and searching capability to improve audit analysis. The privileged administrator configures auditable events, backs-up and manages audit data storage. The TOE provides the privileged administrator with a local circular audit trail, also referred to as the Event Store, and allows for configuration of offload of audit data via TCP syslog to a syslog server in the operational environment so that audit events are not lost when the Event Store reaches capacity and begins to overwrite old events.

5 Assumptions

The following assumptions were made during the evaluation of Cisco 5940 Series Embedded Services Router:

- 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 cannot 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 5940 Series Embedded Services Router:

6.1 Design Documentation

1. Cisco 5940 Series Embedded Services Router Security Architecture Specification, Version 0.2, February 11, 2011
2. Cisco 5940 Series Embedded Services Router Functional Specification, Version 0.4, May 11, 2011
3. Cisco 5940 Series Embedded Services Router TOE Design Specification, Version 0. 3, May 11, 2011
4. Cisco 5940 Series Embedded Services Router Functional Specification Annex B RFC Security Parameter Relevancy, April 2011

6.2 Guidance Documentation

1. Cisco 5940 Series Embedded Services Router Common Criteria Operational User Guidance and Preparative Procedures, Version 0.3, May 2011
2. Release Notes for Cisco IOS Release 15.1(2)GC, January, 31, 2011
3. Cisco 5940 Embedded Services Router Hardware Technical Reference Guide, Last Updated: January 25, 2011
4. Cisco IOS Configuration Fundamentals Configuration Guide, Release 15.1
5. Cisco IOS Security Configuration Guide: Securing User Services, Cisco IOS Release 15.1M&T
6. Network Management Configuration Guide, Cisco IOS Release 15.1M&T
7. Software Configuration Guide for Cisco IOS Release 15.1(2)GC
8. Cisco IOS Security Command Reference

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco 5940 Series Embedded Services Router, ESR-CMP-v1-2, April 2011, Version: 1.2

6.4 Testing

1. Cisco 5940 Series Embedded Services Router Common Criteria Test Documentation, Version 1.2, April 1, 2011
2. Common Criteria Detailed Test Plan, Rev 7, May 7, 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 5940 Series Embedded Services Router, Version 2.0, and June 6, 2011.

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:

1. Identification and Authentication
2. Secure Management
3. VPN and/or Firewall Information Flow Control
4. Intrusion Prevention Services
5. Cryptography
6. 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 5940 Series Embedded Services Router including:

- conduction cooled processor module and air cooled processor module running 15.1(2)GC1t

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco 5940 Series 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 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 5940 Series 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 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 5940 Series Embedded Services Router 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 2 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 high-level design document.

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 2 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 2 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 2 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 2 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 performed a sample of the 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 2 VAN CEM work unit. The evaluation team ensured that the TOE does not contain exploitable flaws or weaknesses in the TOE based upon 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 5940 Series Embedded Services Router Security Target Security Target Security Target, Version 0.07, May 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 5940 Series Embedded Services Router Security Target Part 2 (Proprietary)*, Version 2.0, June 6, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco 5940 Series Embedded Services Router Security Target, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, June 6, 2011.

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

[10] Cisco 5940 Series Embedded Services Router Security Target Security Target, Version 0.07, May 2011.