National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

Cisco ASR9K with CRS-1/3, v4.1.1

Report Number: CCEVS-VR-VID10439-2011
Dated: 9 December 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

Mike Allen (Lead Validator)
The Aerospace Corporation
Columbia, Maryland

Paul Bicknell (Senior Validator)
MITRE Corporation
Bedford, Massachusetts

Common Criteria Testing Laboratory

Tammy Compton
Julie Cowan
Eve Pierre
Quang Trinh
Science Applications International Corporation
Columbia, Maryland

Table of Contents

Mike Allen (Lead Validator) ii
The Aerospace Corporation ii
1 Executive Summary 1
2 Identification 3
2.1 Applicable Interpretations 4
3 Security Policy 5
3.1 Security Audit 5
3.2 Cryptographic Support 5
3.3 Identification and Authentication 5
3.4 Security Management 5
3.5 User Data Protection 6
3.6 Trusted Path/Channel 6
3.7 Protection of the TSF 6
3.8 TOE Access 6
4 Assumptions and Clarification of Scope 7
4.1 Clarification of Scope 7
5 Architectural Information 8
5.1 Physical Scope – ASR 9000 Series (ASR9K) Routers 8
5.2 Physical Scope – CRS-1 Series Routers 9
5.2.1 Physical Scope – CRS-3 Routers 10
6 Documentation 12
6.1 Design Documentation 12
6.2 Guidance Documentation 12
6.3 Life Cycle 14
6.4 Testing 14
7 IT Product Testing 15
7.1 Developer Testing 15
7.2 Evaluation Team Independent Testing 15
8 Evaluated Configuration 16
9 Results of the Evaluation 17
9.1 Evaluation of the Security Target (ASE) 17
9.2 Evaluation of the Development (ADV) 17
9.3 Evaluation of the Guidance Documents (AGD) 18
9.4 Evaluation of the Life Cycle Support Activities (ALC) 18
9.5 Evaluation of the Test Documentation and the Test Activity (ATE) 18
9.6 Vulnerability Assessment Activity (VAN) 19
9.7 Summary of Evaluation Results 19
10 Validator Comments/Recommendations 20
11 Security Target 21
12 Glossary 22
13 Bibliography 23

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 evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Clarification of Scope in Section 4 and the Validator Comments in Section 10.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the CISCO ASR9K with CRS-1/3, v4.1.1. 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 ASR9K with CRS-1/3, v4.1.1 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 November 2011.

The information in this report is largely derived from the Security Target (ST), Evaluation Technical Reports (ETR) and the 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 3 (EAL 3) augmented with ALC_FLR.2 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 ASR9K with CRS-1/3, v4.1.1 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 3 augmented by ALC_FLR.2. All security functional requirements are derived from Part 2 of the Common Criteria.

The TOE is a purpose-built, wide-area network (WAN) routing platform that provides basic security functionality including network Access Control Lists, administrative security, and firewall functionality. The TOE includes a number of chassis options: the ASR 9006 and ASR 9010, the CRS-1 4-slot, CRS-1 8-slot, and CRS-1 16-slot single shelf options, multiple shelf/chassis options of the CRS-1 16-slot, as well as upgraded switching fabric (CRS-3) models including CRS-3 4-slot, CRS-3 8-slot, CRS-3 16-slot single shelf options and multiple shelf/chassis options of the CRS-3 16-slot.

A validation team from CCEVS monitored the activities of the evaluation team, reviewed 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 concluded that SAIC's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of SAIC in the evaluation technical report are consistent with the evidence produced.

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, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 Aggregation Services Router (ASR) 9000 series, with IOS XR operating system version 4.1.1 and the Carrier Routing System (CRS) routers CRS-1 and CRS-3
Protection Profile	N/A
Security Target	*CISCO ASR9K with CRS-1/3, v4.1.1 Security Target*, version 1.0, November 1, 2011
Dates of evaluation	August 2010 through November 2011
Evaluation Technical Report	*Evaluation Technical Report for the CISCO ASR9K with CRS-1/3, (Non-Proprietary)*, Version 2.0, November 30, 2011 *Evaluation Technical Report for the CISCO ASR9K with CRS-1/3, (Proprietary)*, Version 2.0, November 7, 2011
Conformance Result	Part 2 extended conformant and EAL3 Part 3 augmented with ALC_FLR.2
Common Criteria version	Common Criteria for Information Technology Security Evaluation Version 3.1R3, July 2009 and all applicable NIAP and International Interpretations effective on August 30, 2010
Common Evaluation Methodology (CEM) version	CEM version 3.1R3 dated July 2009 and all applicable NIAP and International Interpretations effective on August 30, 2010
Sponsor	CISCO Systems, Inc.,
Developer	CISCO Systems, Inc.,
Common Criteria Testing Lab	SAIC Inc., Columbia, MD
Evaluators	Tammy Compton, Julie Cowan, Eve Pierre, and Quang Trinh of SAIC, Columbia, Maryland

Validation Team	Paul Bicknell of MITRE Corporation and Mike Allen of The Aerospace Corporation

2.1 Applicable Interpretations

The following NIAP and International Interpretations were determined to be applicable when the evaluation started.

NIAP Interpretations

None.

International Interpretations

None.

3 Security Policy

This section summaries the security functionality of the TOE:

Security Audit
Cryptographic Support
Identification and Authentication
Security Management
User Data Protection
Trusted Path/Channel
Protection of the TSF
TOE Access

3.1 Security Audit

The TOE can audit events related to cryptographic functionality, information flow control enforcement, identification and authentication, and administrative actions. The IOS generates an audit record for each auditable event. Administrators can search, view and manage the set of auditable events.

3.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality, including AES, Triple DES and DSA, to support SSHv2, SNMPv3, and SSL. This cryptography is stated by the manufacturer to be conformant to the applicable FIPS publications; however, neither the algorithm implementations nor the embodiment have been formally validated[1].

3.3 Identification and Authentication

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI administrative interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality. In addition, the TOE supports local and remote identification and authentication of TOE users. Unsuccessful authentication attempts can be limited based on authorized administrator configuration.

3.4 Security Management

The Management Plane Protection (MPP) feature in Cisco IOS XR software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows an administrator to designate one or more router interfaces as management interfaces. Once a management interface is configured and MPP is enabled,

[1] For CRS, all cryptography is embodied within software modules. For ASR9000, the embodiment may include both software and hardware cryptographic modules. FIPS 140 validation has not been obtained for any embodiment.

management traffic may only enter the device through this interface. The management interface is restricted to authorized administrators and provides the ability to manage the security functions and users of the TOE. The pre-defined management roles can be augmented with additional fine-grained defined roles to provide role separation.

3.5 User Data Protection

The TOE enforces the following information flow control policies:
Unauthenticated TOE services—the TOE mediates all information flows to and from the TOE itself. The TOE has the ability to permit or deny information flows based on the characteristics of the information flow.
Unauthenticated information flow—the TOE mediates all information flows through the TOE for unauthenticated information flows.

3.6 Trusted Path/Channel

The TOE establishes a trusted path between itself and the remote management station used by the administrators to manage the TOE. This Trusted path is secured using an SSHv2[2], SSL, or SNMPv3 secure connection.

3.7 Protection of the TSF

The TOE is capable of preserving a secure state when software or hardware failures occur. The TOE provides manual and automatic recovery mechanisms. In addition, the TOE protects all TSF data from unauthorized modification and disclosure during transmission. The TOE provides hardware failover for hardware or software faults within the TSF for configurations that include dual RPs or dual RSPs.

3.8 TOE Access

The TOE provides the capability for the TSF to determinate when there is user inactivity and terminates the session. A user will have to re-authenticate and start a new session. Advisory user interface banners can be configured.

[2] IOS XR includes support for SSHv1 for backward compatibility, but for security reasons that support should be disabled in the evaluated configuration of the TOE.

4 Assumptions and Clarification of Scope

The assumptions in the following paragraphs were made during the evaluation of CISCO ASR9K with CRS-1/3, v4.1.1.

- The Administrator ensures there are no general purpose computing or storage repository capabilities (e.g., compilers, editors, web servers, database servers or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
- The TOE can utilize external RADIUS or TACACS+ authentication servers.

4.1 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. Note that:

- The timestamps of the events in the main syslog buffer on the TOE do not contain the year, so care must be taken during searches based on the date. The administrator must first examine the start and end of the syslog to ensure that the dates do not span a period greater than 12 months.
- The Cryptography used by the product has not been independently certified. The Cryptography of the product is vendor certified to operate correctly.
- Administrators must be careful when configuring the audit functionality. There are no alerts or warnings should the audit trail become full. Audit data will be lost should this occur.

5 Architectural Information

The TOE consists of the ASR 9000 Series Routers (ASR9K), and the CRS-1 and CRS-3 routers, each containing the IOS XR V4.1.1 Operating System and a primary command line interface (CLI). Alternate administrative interfaces include SNMPv3 (which is primarily used for monitoring but does provide a limited ability to administer the router and change configuration) and an Application Programming Interface (API) that allows complex router configurations to be added or changed using XML-formatted text in place of a series of individual CLI commands.

Route Processors (RPs) within CRS routers and Route Switch Processors (RSPs) within the ASR9K routers provide the advanced packet routing capabilities. The processors provide the monitoring, managing, and configuring services for the TOE itself. The CLI is provided, and TOE administration is performed, within the processors. In addition the RPs and RSPs negotiate and maintain encryption methods, and encryption keys between the TOE and external IT entities.

Shared Port Adapters (SPAs) provide the physical interfaces for TOE connectivity to the connected network including copper, channelized, POS, and Ethernet.

Outside the TOE physical boundaries but inside the relevant IT environment, the TOE will generally require one or more of an SSH client, an SNMPv3 engine/server, and/or a suitable Operations Support System (OSS) that provides secure XML management using the Cisco XML API, in order to support administration of the ASR9000 series or CRS series routers. In addition, an external RADIUS or TACACS+ authentication server may be used to provide authentication services to administrative users of the TOE.
The Management Plane Protection (MPP) feature in Cisco IOS XR software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows an administrator to designate one or more router interfaces as management interfaces. Once a management interface is configured and MPP is enabled, management traffic may only enter the device through this interface. The management interface is restricted to authorized administrators and provides the ability to manage the security functions and users of the TOE. The pre-defined management roles can be augmented with additional fine-grained defined roles to provide role separation.

5.1 Physical Scope – ASR 9000 Series (ASR9K) Routers

The ASR9K Series consists of two (2) chassis options, the Cisco ASR 9000 Series 6-Slot Chassis (ASR-9006) with 4 line cards and the Cisco ASR 9000 Series 10-Slot Chassis (ASR-9010) with 8 line cards. Both contain two slots dedicated for dual redundant Route Switch Processors (RSPs), modular fans, and AC or DC power supplies. Each Chassis contains a minimum of one RSP, nominally two per chassis. The RSPs provide routing engine as well as switching fabric with active non-blocking mode for redundant RSPs.

The following Ethernet modules are available for plug-in to either chassis:

- 40-port Gigabit Ethernet,
- 4-port 10GBps Ethernet,

- 8-port 10Gbps Ethernet line cards, and
- 2-port 10 Gigabit Ethernet + 20-port Gigabit Ethernet.

Each of the line card types is available in three "scale types" (High Queue, Medium Queue, and Low Queue) supporting differing numbers of simultaneous packet queues and related functionality.

A complete list of Ethernet line card variants is as follows:

- A9K-40GE-L
- A9K-40GE-B
- A9K-40GE-E
- A9K-4T-L
- A9K-4T-B
- A9K-4T-E
- A9K-8T/4-L
- A9K-8T/4-B
- A9K-8T/4-E
- A9K-2T20GE-L
- A9K-2T20GE-B
- A9K-2T20GE-E
- A9K-8T-L
- A9K-8T-B
- A9K-8T-E
- A9K-16/8T-B

Additionally, there is support for non-Ethernet interfaces in the Shared Port Adapter (SPA) form factor that is common to other Cisco routers. These SPAs are installed into the SPA Interface Processor line card A9K-SIP-700.

5.2 Physical Scope – CRS-1 Series Routers

There are two CRS-1 Series form factors: LCC and FCC.

The CRS-1 Series Router, LCC consists of three (3) chassis options: the Cisco CRS-1 4-slot chassis, the Cisco CRS-1 8-slot chassis, and the Cisco CRS-1 16-slot chassis.

Each CRS-1 16-Slot Line-Card Chassis includes:

- Two route processors (CRS-16-RP)
- Two CRS-1 16 fan controllers
- Eight CRS-1 16 fabric cards
- Two Power Shelves (either DC, AC type Wye, AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

Optional items include:

- 16 CRS-1 line cards
- 16 CRS-1 PLIMs.

Supported line cards for CRS-1 comprise:

- 1-port OC-768c/STM-256c packet over Synchronous Optical Network (POS) - 1OC768-POS-SR
- 1-port OC-768 DPSK+ (C-band) DWDM PLIM - 1OC768-DPSK/C 8-port 10 Gigabit Ethernet - 8-10GBE or 8-10GBE-WL-XFP
- 4-port 10 Gigabit Ethernet - 4-10GBE-WL-XFP
- CRS1-SIP-800 Carrier Card - CRS1-SIP-800
- 4-Port OC-3/STM-1 POS SPA
- 8-Port 1 Gigabit Ethernet SPA
- 1-port OC-768c/STM-256c Tunable WDMPOS
- 4-port 10GE Tunable WDMPHY
- 20-port 1 Gigabit Ethernet Flexible interface - 20-1GE-FLEX
- 1-port 100 Gigabit Ethernet - 1X100GBE
- 2-port.10 Gigabit Ethernet WAN/LAN Flexible - 2-10GE-WL-FLEX
- 14-port 10 Gigabit Ethernet LAN/WAN - 14X10GBE-WL-XFP
- 20-port 10 Gigabit Ethernet LAN/WAN - 20X10GBE-WL-XFP

The CRS-1 Series Router, FCC form factor, consists of one (1) chassis option: the Cisco CRS-1 24-Slot FCC. The Cisco CRS-1 24-Slot FCC is part of the CRS-1 16-slot multi-chassis system and includes:

- Two Cisco CRS-1 fan controllers (part number CRS-FCC-SC-22GE)
- Eight Cisco CRS-1 S2 fabric cards (part number CRS-FCC-SFC)
- Two power shelves (DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

5.2.1 Physical Scope – CRS-3 Routers

The CRS-3 routers are physically identical to the CRS-1 routers other than the revised switching fabric. The TOE physical boundaries are the same between CRS-1 and CRS-3, but all the part numbers/nomenclature are different due to the improved switching fabric—therefore the CRS-1 and CRS-3 routers have been described separately.
There are two CRS-3 Series form factors: LCC and FCC.

The CRS-3 Series Router, LCC consists of three (3) chassis options: the Cisco CRS-3 4-slot chassis, the Cisco CRS-3 8-slot chassis, and the Cisco CRS-3 16-slot chassis.

Each Cisco CRS-3 16-slot line card chassis includes:

- Two route processors (CRS-16-RP)
- Two Cisco CRS-1 16 slot system fan controllers

- Eight Cisco CRS-3 16 slot system fabric cards
- Two power shelves (either DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

Optional items include:

- 16 Cisco CRS-1 line cards or CRS-3 line cards
- 16 Cisco CRS-1 PLIMs or CRS-3 PLIMs.

Supported line cards for CRS-3 under IOS XR v4.1.1 are:

- 1-port OC-768c/STM-256c packet over SONET (PoS) - 1OC768-POS-SR
- 1-port OC-768 DPSK+ (C-band) DWDM PLIM - 1OC768-DPSK/C
- 8-port 10 Gigabit Ethernet (GE) - 8-10GBE or 8-10GBE-WL-XFP
- 4-port 10 GE - 4-10GBE-WL-XFP
- 1-port OC-768c/STM-256c tunable WDMPoS
- 4-port 10GE tunable WDMPHY
- 14-port 10GE LAN/WAN PHY - 14X10GBE-WL-XFP
- 20-port 10GE LAN/WAN PHY - 20X10GBE-WL-XFP
- 1-port 100GE - 1X100GBE
- Cisco CRS-1-SIP-800 Carrier Card - CRS1-SIP-800
- 2- and 4-port OC-3c/STM-1c PoS shared port adapters (SPAs)
- 1-, 2-, and 4-port OC-48c/STM-16c PoS/RPR SPAs
- 1-port OC-192c/STM-64c PoS/RPR SPA
- 1-port 10GE SPA
- 2-port and 4-port Clear Channel T3/E3 SPAs
- 2-port, 4-port, and 8-port OC-12c/STM-4 PoS SPAs
- 2-port, 5-port, 8-port, and 10-port GE SPAs
- 1-port 10GE LAN/WAN-PHY SPA
- 20-port GE Flexible Interface Module - 20-1GE-FLEX
- 2-port 10GE WAN/LAN-PHY flexible interface module - 2-10GE-WL-FLEX .

The CRS-3 Series Router, FCC consists of one (1) chassis option: the Cisco CRS-3 24-Slot FCC. The Cisco CRS-3 24-Slot FCC is part of the CRS-3 16-slot multi-chassis system and includes:

- Two Cisco CRS-3 fan controllers (part number CRS3-FCC-SC-22GE)
- Eight Cisco CRS-3 S2 fabric cards (part number CRS3-FCC-SFC)
- Two power shelves (DC, AC type Wye, or AC type Delta)
- Two alarm cards
- Two fan trays
- One fan filter.

6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco ASR9K with CRS-1/3, v4.1.1. Only those documents identified in the Guidance Documentation section are provided to customers.

6.1 Design Documentation

1. Cisco ASR9K with CRS-1/3, v4.1.1 Security Architecture Specification, Version 0.3, September 27, 2010
2. Cisco ASR9K with CRS-1/3, v4.1.1 Functional Specification, Version 0.5, November 1, 2011
3. Cisco ASR9K with CRS-1/3, v4.1.1 TOE Design Specification, Version 0.5, September 27, 2011
4. Cisco ASR9K with CRS-1/3, v4.1.1 Functional Specification Annex B RFC Security Parameter Relevancy, Version 0.3, September 27, 2011

6.2 Guidance Documentation

1. Cisco ASR9K with CRS-1/3, v4.1.1 Common Criteria Operational User Guidance and Preparative Procedures, Version 0.7, November 2011
2. Cisco ASR 9000 Series Aggregation Services Routers, Release 4.0 (also applicable to Release 4.1.1)
   - **[ASR-GS]** Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide, Release 4.0
   - **[ASR-SC]** Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide, Release 4.0
   - **[ASR-SM]** Cisco ASR 9000 Series Aggregation Services Router System Management Configuration Guide, Release 4.0
3. Cisco CRS Router, Release 4.0 (also applicable to Release 4.1.1)
   - **[CRS-GS]** Cisco IOS XR Getting Started Guide for the Cisco CRS-1 Router, Release 4.0
   - **[CRS-SC]** Cisco IOS XR System Security Configuration Guide for the Cisco CRS Router, Release 4.0
   - **[CRS-SM]** Cisco IOS XR System Management Configuration Guide for the Cisco CRS Router, Release 4.0
4. ASR 9000 Command References

- Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Command Reference
- Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router L2VPN and Ethernet Services Command Reference
- Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router MPLS Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router Netflow Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router System Management Command Reference, Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router System Monitoring Command Reference,\n Release 4.0
- Cisco ASR 9000 Series Aggregation Services Router System Security Command Reference, Release 4.0

5. CRS Command References

- Cisco IOS XR Carrier Grade NAT Command Reference for the Cisco CRS Router
- Cisco IOS XR Interface and Hardware Component Command Reference for the Cisco CRS Router
- Cisco IOS XR IP Addresses and Services Command Reference for the Cisco CRS Router
- Cisco IOS XR Modular Quality of Service Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR MPLS Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR Multicast Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR Netflow Command Reference for the Cisco CRS Router, Release 4.0

- Cisco IOS XR Routing Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR System Monitoring Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR System Security Command Reference for the Cisco CRS Router, Release 4.0
- Cisco IOS XR Virtual Private Network Command Reference for the Cisco CRS Router
- Cisco IOS XR System Management Command Reference for the Cisco CRS Router, Release 4.0

6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco ASR9K with CRS-1/3, v4.1.1, ASR9K-CRS-CMP-v1, November 2011, Version: 1.3

6.4 Testing

1. ASR 9000 Series, CRS-1, 3 Common Criteria Test Documentation, Version 1.2, 09/23/2011
2. Project ASR9K Common Criteria Detailed Software Test Plan, Revision 0.2, 09/23/2011
1. Project CRS Common Criteria Detailed Software Test Plan, Revision 0.6, 09/23/2011

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 ASR9K with CRS-1/3, v4.1.1, Version 2.0, November 7, 2011.

7.1 Developer Testing

At EAL3, 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. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. User Data Protection
6. Trusted Path/Channel
7. Protection of the TSF
8. TOE Access

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to 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 the Cisco Aggregation Services Router (ASR) 9000 series, with IOS XR operating system version 4.1.1 plus the following SMUs: asr9k-p-4.1.1.CSCtq56564, asr9k-p-4.1.1.CSCtr86240, and asr9k-p-4.1.1.CSCtq59879, and the Carrier Routing System (CRS) routers CRS-1 and CRS-3, with IOS XR operating system version 4.1.1 plus the following SMUs: hfr-px-4.1.1.CSCtq21686.pie, hfr-px-4.1.1.CSCtq59879.pie, hfr-px-4.1.1.CSCtr70418.pie, hfr-px-4.1.1.CSCtq16133.pie, hfr-px-4.1.1.CSCtr16132.pie.

To use the product in the evaluated configuration, the product must be configured as specified in the *Cisco ASR9K with CRS-1/3, v4.1 Common Criteria Operational User Guidance and Preparative Procedures*, November 2011 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 EAL3 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 Aggregation Services Router (ASR) 1000 Series TOE to be Part 2 extended, and to meet the Part 3 Evaluation Assurance Level (EAL 3) 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 ASR9K with CRS-1/3, v4.1 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 3 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 3 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 3 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 3 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 3 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 3 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's observations support the evaluation team's conclusion that the CISCO ASR9K with CRS-1/3, v4.1.1 meets the claims stated in the Security Target. The validation team also wishes to add the following clarification about the use of the product.

- The Cryptography used by the product has not been independently certified. The Cryptography of the product is solely vendor certified to operate correctly. No FIPS evaluations of the cryptography have been performed.
- Administrators must be careful when configuring the audit functionality. There are no alerts or warnings should the audit trail become full. Audit data will be lost should this occur.

11 Security Target

The Security Target is identified as *Cisco ASR9K with CRS-1/3, v4.1.1 Security Target, Version 1.0,* dated November 1, 2011. 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 3 augmented with ALC_FLR.2.

12 Glossary

The following abbreviations and definitions are used throughout this document:

CC ……..……Common Criteria
EAL3 ……..……Evaluation Assurance Level 3
IT ……..Information Technology
NIAP ……..……..National Information Assurance Partnership
PP ……Protection Profile
SF ……..……Security Function
SFP ……..……..Security Function Policy
ST ……Security Target
TOE ……..……Target of Evaluation
TSC ……..……TSF Scope of Control
TSF ……..……..TOE Security Functions
TSFI ……TSF Interface
TSP ……..……TOE Security Policy

- **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, Revision 3, dated: July 2009.

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

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

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 3, 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 ASR9K with CRS-1/3, Part 1 (Non-Proprietary),* Version 2.0, November 30, 2011.

[7] Science Applications International Corporation. *Evaluation Technical Report for the Cisco ASR9K with CRS-1/3, Part 2 (Proprietary),* Version 2.0, November 7, 2011.

[8] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco ASR9K with CRS-1/3, v4.1, ETR Part 2 Supplement (SAIC and Cisco Proprietary),* Version 3.0, November 7, 2011. NOTE: This document was used only to develop summary information regarding the testing performed by the CCTL.

[9] Cisco ASR9K with CRS-1/3, v4.1.1 Series Security Target, Version 1.0, November 1, 2011.