# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme
# Validation Report

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

## Aggregation Services Router (ASR) 1000 Series

**Report Number:** CCEVS-VR-10361-2011
**Dated:** 27 June 2011
**Version:** 0.2

**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

**Kenneth Elliott**
*The Aerospace Corporation*
***Columbia, MD***

**Olin Sibert**
*Orion Security Solutions, Inc.*
***McLean, VA***

## Common Criteria Testing Laboratory

Tammy Compton
Gary Grainger
Katie Sykes
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 Aggregation Services Router (ASR) 1000 Series 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 May 2011. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by SAIC. The evaluation determined that the product is both **Common Criteria Part 2 Extended and Part 3 Conformant**, and meets the assurance requirements of EAL 4 augmented with ALC_FLR.2.

The Cisco ASR 1000 Series Router (ASR 1002, ASR 1002f, ASR 1004, ASR 1006) delivers embedded hardware acceleration for multiple Cisco IOS® XE Software services. In addition, the Cisco ASR 1000 Series Router features redundant Route and Embedded Services Processors, as well as software-based redundancy. In support of the routing capabilities, the Cisco ASR 1000 Series Router provides IPSec connection capabilities for VPN enabled clients connecting through the Cisco ASR 1000 Series Router. The Cisco ASR 1000 Series Router also supports firewall capabilities. The ASR 1000 Series Router is a single-device security and routing solution for protecting the WAN entry point into the network. Zone-based firewall allows grouping of physical and virtual interfaces into zones to simplify logical network topology. The creation of these zones facilitates the application of firewall policies on a zone-to-zone basis, instead of having to configure policies separately on each interface.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 3) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 3). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team monitored the activities of the evaluation team, observed evaluation testing activities, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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

The technical information included in this report was obtained from the Cisco Aggregation Services Router (ASR) 1000 Series 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 Profiles from which functional requirements were drawn.
- 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 Aggregation Services Router (ASR) 1000 Series running IOS XE 2.4.2t |
| **Protection Profile** | Functional compliance to the following:<br>U.S. Government Router Protection Profile For Medium Robustness Environments, version 1.1, July 25, 2007<br>U.S. Government Virtual Private Network (VPN) Boundary Gateway Protection Profile For Medium Robustness Environments, version 1.2, January 30, 2009<br>U.S. Government Protection Profile for Traffic Filter Firewall For Medium |

| Item | Identifier |
|---|---|
|  | Robustness Environments, version 1.1, July 25, 2007 |
| **ST:** | Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version 0.19, May 2011 |
| **Evaluation Technical Report** | Evaluation Technical Report For the Cisco Aggregation Services Router (ASR) 1000 Series (Proprietary), Version 2.0, May 11, 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 |
| **Sponsor** | Cisco Systems, Inc |
| **Developer** | Cisco Systems, Inc |
| **Common Criteria Testing Lab (CCTL)** | SAIC, Columbia, MD |
| **CCEVS Validators** | Kenneth Elliott, The Aerospace Corporation, Columbia, MD<br>Olin Sibert, Orion Security Solutions, Inc., McLean, VA |

# 3 Architectural Information

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

## 3.1 TOE Introduction

This section provides an overview of the Aggregation Services Router (ASR) 1000 Series Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 2-RU, 4-RU, and 6-RU form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Embedded Services Processor (ESP): The Cisco ASR 1000 Series ESPs are responsible for the data-plane processing tasks, and all network traffic flows through them.
- Route Processor (RP): The Cisco ASR 1000 Series RPs provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the Cisco ASR 1000 Series Aggregation Services.
- Shared Port Adaptors (SPAs): Used for connecting to networks. These SPAs interface with the TOE to provide the network interfaces that will be used to communicate on the network.

**Table 1: TOE Component Descriptions**

| Hardware Model | Cisco ASR 1002f | Cisco ASR 1002 | Cisco ASR 1004 | Cisco ASR 1006 |
|---|---|---|---|---|
| **Software Model** | Cisco IOS XE Version 2.4.2t | Cisco IOS XE Version 2.4.2t | Cisco IOS XE Version 2.4.2t | Cisco IOS XE Version 2.4.2t |

| | | | | |
|---|---|---|---|---|
| **Size** | 2-Rack Units | 2-Rack Units | 4-Rack Units | 6-Rack Units |
| **Power** | DC power: 590W<br>AC Power: 560W | DC power: 590W<br>AC Power: 560W | DC power: 1020W<br>AC Power: 960W | DC power: 1700W<br>AC Power: 1600W |
| **Supported ESPs** | Integrated ESP | ESP5<br>ESP10 | ESP10<br>ESP20 | Dual ESP10<br>Dual ESP20 |
| **Supported ESP Throughput** | 2.5 Gbps | ESP5 – 5 Gbps<br>ESP10 – 10 Gbps | ESP10 – 10 Gbps<br>ESP20 – 20 Gbps | ESP10 – 10 Gbps<br>ESP20 – 20 Gbps |
| **Supported ESP Processors** | Freescale 8543 | Freescale 8543 (both ESPs) | Freescale 8543 (both ESPs) | Freescale 8543 (both ESPs) |
| **Supported RPs** | Integrated RP | Integrated RP | RP1<br>RP2 | Dual RP1<br>Dual RP2 |
| **Supported RP Processors** | Freescale 8548 | Freescale 8548 | RP1: Freescale 8548<br>RP2: Intel Wolfdale-DP | RP1: Freescale 8548<br>RP2: Intel Wolfdale-DP |
| **Supported SPAs (all TOE model support all SPAs)** | Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1)<br>Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter (SPA-4XCT3/DS0)<br>Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter (SPA-2XCT3/DS0)<br>Cisco 1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter (SPA-1XCHSTM1/OC3)<br>Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3)<br>Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter (SPA-4XT3/E3)<br>Cisco 4-Port Serial Interface Shared Port Adapter (SPA-4XT-Serial)<br>Cisco 4-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-4X1FE-TX-V2)<br>Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-8X1FE-TX-V2)<br>Cisco 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE-V2)<br>Cisco 5-Port Gigabit Ethernet Shared Port Adapter (SPA-5X1GE-V2)<br>Cisco 8-Port Gigabit Ethernet Shared Port Adapter (SPA-8X1GE-V2)<br>Cisco 10-Port Gigabit Ethernet Shared Port Adapter (SPA-10X1GE-V2)<br>Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter (SPA-1X10GE-L-V2)<br>Cisco 2-Port OC3c/STM-1c POS Shared Port Adapter (SPA-2XOC3-POS)<br>Cisco 4-Port OC3c/STM-1c POS Shared Port Adapter (SPA-4XOC3-POS)<br>Cisco 8-port OC3/STM4 POS Shared Port Adapter (SPA-8XOC3-POS)<br>Cisco 1-Port OC12c/STM-4c POS Shared Port Adapter (SPA-1XOC12-POS)<br>Cisco 2-port OC12/STM4 POS Shared Port Adapter (SPA-2XOC12-POS)<br>Cisco 4-port OC12/STM4 POS Shared Port Adapter (SPA-4XOC12-POS)<br>Cisco 8-port OC12/STM4 POS SPA Shared Port Adapter (SPA-8XOC12-POS)<br>Cisco 1-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-1XOC48-POS/RPR)<br>Cisco 2-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-2XOC48POS/RPR)<br>Cisco 4-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-4XOC48POS/RPR)<br>Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics (SPA-OC192POS-XFP) | | | |
| **SPA Slots** | 1 SPA slot | 3 SPA slots | 8 SPA slots | 12 SPA slots |
| **Interfaces** | Port Adapter Interface<br>Console Port<br>Auxiliary Port<br>10/100 BITS | Port Adapter Interface (3)<br>Console Port<br>Auxiliary Port<br>10/100 BITS | Port Adapter Interface (8)<br>Console Port<br>Auxiliary Port<br>10/100 Management | Port Adapter Interface (12)<br>Console Port<br>Auxiliary Port (2)<br>10/100 BITS |

| | | | | |
|---|---|---|---|---|
| | Ethernet Port<br>10/100 Management Ethernet Port<br>USB Port<br>GigE Ports (4) | Ethernet Port<br>10/100 Management Ethernet Port<br>USB Port<br>GigE Ports (4) | Ethernet Port<br>10/100 BITS Ethernet Port (1)<br>USB Ports (2) | Ethernet Port (2)<br>10/100 Management Ethernet Port (2)<br>USB Ports (4) |
| **Hardware Redundancy Supported?** | Not supported | Not supported | Not supported | Supported |

## 3.2 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Aggregation Services Router (ASR) 1000 Series Router. The TOE is comprised of the following:

**Table 2: Physical Scope of the TOE**

| TOE Configuration | Hardware Configurations | Software Version |
|---|---|---|
| ASR 1002f | No configuration options | IOS XE 2.4.2t software running on a hardened version of Linux Kernel 2.6.8. |
| ASR 1002 | ESP5 or ESP10 | IOS XE 2.4.2t software running on a hardened version of Linux Kernel 2.6.8. |
| ASR 1004 | RP 1 or RP 2<br>ESP10 or ESP20 | IOS XE 2.4.2t software running on a hardened version of Linux Kernel 2.6.8. |
| ASR 1006 | RP 1 or RP 2<br>Dual ESP10 or ESP20 | IOS XE 2.4.2t software running on a hardened version of Linux Kernel 2.6.8. |

As identified above, there are several configurations available for each TOE hardware model (ASR 1002, ASR 1002f, ASR 1004, ASR 1006). Each model supports one or more Embedded Services Processors (ESP) and one or more Router Processors (RP). Additionally, each TOE hardware model is configured to include one or more SPAs to facilitate network connectivity. The following table identifies the number of SPAs supported by each TOE hardware model and identifies the SPAs included within the TOE.

**Table 3: Physical Scope of the TOE**

| TOE Configuration | SPA Slots | TOE SPAs |
|---|---|---|
| ASR 1002f | 1 SPA slot | Cisco 8-Port Channelized T1/E1 Shared Port Adapter |
| ASR 1002 | 3 SPA slot | Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter |

| | | |
|---|---|---|
| ASR 1004 | 8 SPA slot | Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter<br>Cisco 1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter<br>Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter<br>Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter<br>Cisco 4-Port Serial Interface Shared Port Adapter<br>Cisco 4-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter<br>Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter<br>Cisco 2-Port Gigabit Ethernet Shared Port Adapter<br>Cisco 5-Port Gigabit Ethernet Shared Port Adapter<br>Cisco 8-Port Gigabit Ethernet Shared Port Adapter<br>Cisco 10-Port Gigabit Ethernet Shared Port Adapter<br>Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter<br>Cisco 2-Port OC3c/STM-1c POS Shared Port Adapter<br>Cisco 4-Port OC3c/STM-1c POS Shared Port Adapter<br>Cisco 8-port OC3/STM4 POS Shared Port Adapter<br>Cisco 1-Port OC12c/STM-4c POS Shared Port Adapter<br>Cisco 2-port OC12/STM4 POS Shared Port Adapter<br>Cisco 4-port OC12/STM4 POS Shared Port Adapter<br>Cisco 8-port OC12/STM4 POS SPA Shared Port Adapter<br>Cisco 1-port OC48/STM16 POS/RPR Shared Port Adapter<br>Cisco 2-port OC48/STM16 POS/RPR Shared Port Adapter<br>Cisco 4-port OC48/STM16 POS/RPR Shared Port Adapter<br>Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics |
| ASR 1006 | 12 SPA slot | |

The following provides a functional description of each sub-component.

### 3.2.1 Embedded Services Processor (5Gbps, 10Gbps, 20Gbps)

The ESPs are responsible for the data-plane processing tasks, and all network traffic flows through them. Packets arrive to the ESPs from the network. Each packet is decoded, interpreted, processed and forwarded, as necessary, by the ESP. The ESP performs all baseline packet routing operations, including MAC classification, Layer 2 and Layer 3 forwarding, quality-of-service (QoS) classification, policing and shaping, security access control lists (ACLs), VPN, load balancing, and NetFlow. The ESPs contain a cryptographic co-processor. This co-processor is dedicated to providing cryptographic acceleration for cryptographic operations within the ASR 1000.

### 3.2.2 Route Processor (RP1, RP2)

The RPs within the ASR 1000 provides the advanced packet routing capabilities of the ASR 1000 Series Router. The RPs provide the monitoring, managing, and configuring services for the TOE itself. All TOE administration is performed within the RPs. The administrative CLI interface is provided by the Route Processors. The RPs also negotiate and maintain IPSec authentication, encryption methods, and encryption keys between the TOE and external IT entities.

### 3.2.3 Shared Port Adaptors

SPAs provide the physical interfaces for TOE connectivity to the connected network including copper, channelized, POS, and Ethernet

# 4 Security Policy

This section summaries the security functionality of the TOE:

1. Identification & Authentication
2. Security Management
3. VPN, Router, and/or Firewall Information Flow Control
4. Trusted Channel/Path
5. Cryptography
6. Security Audit
7. Availability

### 4.1.1 Identification & Authentication

The ASR performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the ASR. Device-level authentication allows the ASR 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 ASR provides authentication services for administrative users wishing to connect to the ASRs secure CLI administrative interface. The TOE requires authorized administrators to authenticate prior to being granted access to any of the management functionality.

### 4.1.2 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session via terminal server or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all audit functionality of the TOE; all TOE cryptographic functionality; and the information flow control policies enforced by the TOE. The TOE supports three separate administrative roles: Cryptographic Administrator, Audit Administrator and Security Administrator. The Cryptographic Administrator is responsible for the configuration and maintenance of cryptographic elements related to the establishment of secure connections to and from the TOE. The Audit Administrator is responsible for the regular review of the TOE’s audit data. The Security Administrator is responsible for all other administrative tasks.

When an administrative session is initially established, the TOE displays a Security Administrator configurable warning banner. This is used to provide any information deemed necessary by the Security Administrator. The TOE supports several scenarios in which the administrative session is either locked out or terminated, as follows;

- The TOE allows an administrator to lock out her administrative session on demand.
- The TOE locks administrative sessions based on a configured period of inactivity.
- The TOE terminates the administrative session after a configurable time interval of session inactivity occurs.

### 4.1.3 VPN, Router, and/or Firewall Information Flow Control

The TOE enforces several information flow control policies, including:

- VPN services
- Unauthenticated TOE services
- Unauthenticated information flow

Each of these enforced information flows are further discussed below.

#### 4.1.3.1 VPN services

The VPN process includes remote device authentication, negotiation of specific cryptographic parameters for the session, and providing a secure connection from and to the remote device. For inbound or outbound connections with external IT entities that are capable of supporting VPN (e.g., a peer ASR 1000 series router, a VPN Peer), the TOE will establish a secure connection. For other inbound or outbound traffic a secure connection will not be established.

#### 4.1.3.2 Unauthenticated TOE services

The Cisco ASR 1000 Series Routers mediate all information flows to and from the ASR itself. The TOE has the ability to permit or deny information flows based on the characteristics of the information flow. By examining the information flows to the TOE itself, the ASR is able to provide specific TOE services to requesting unauthenticated entities. The TOE services that are available to unauthenticated entities are configurable by the Security Administrator and must include, ICMP. All other TOE services are only available to authenticated entities.

#### 4.1.3.3 Unauthenticated information flow

The Cisco ASR 1000 mediates all information flows through the ASR for unauthenticated information flows. The TOE provides the ability to classify all data flows into zones. Configurable allow or deny rule sets are applied to each information flow on a zone by zone basis. All security attributes are inspected based on the configurable rule set of the information flow. The TOE makes the decision to allow or deny unauthenticated information flows based on the configured information flow rule set. The ASR generates and maintains “state” information for all approved connections mediated by the TOE. The “state” information is used to monitor the status of an approved connection and validate incoming packets received as part of an approved connection.

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with random information. Residual data is never transmitted from the TOE. Additionally, The TOE maintains counters of the number of the connections through the TOE. When the TOE's counters exceed the maximum sessions, the TOE will take actions to reduce the number of connections.

### 4.1.4 Trusted Path/Channel

The TOE establishes a trusted path between the TOE and the remote management station used by the administrators to manage the TOE. This Trusted path is secured using an SSHv2 secure connection. All remote administration occurs through the SSHv2 secure trusted path. Alternatively, the TOE supports local administration through a directly connected management station.

The ASR establishes a trusted channel between itself and peer IT devices. Between the ASR and peer routers, network control information is exchanged via trusted channels to allow dynamic connection establishment and packet routing. Network control information consists of specific requests and instructions that include destination address, routing controls, and signaling information. Trusted channels are secured via IPSec encryption.

### 4.1.5 Cryptography

The TOE provides cryptography in support of other ASR security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 overall Level 2 and Level 3 for sections 3 and 10. The ASR provides cryptography in support of VPN connections. The cryptographic services provided by the TOE in support of IPSec include:

**Table 4: IPSec Related Cryptography**

| Cryptographic Method | Use within IPSec |
|---|---|
| Internet Key Exchange | Used to establish initial IPSec session. |
| SP 800-56 Key Exchange | Used in IPSec session establishment. |
| Group Domain of Interpretation | Used in IPSec session establishment. |
| RSA Digital Signatures | Used in IPSec session establishment. |
| ANSI X9.31 PRNG | Used in IPSec session establishment. |
| SHS | Used to provide IPSec traffic integrity verification. |
| AES | Used to encrypt IPSec session traffic. |

The TOE also provides cryptography in support of secure administration. The following table identifies the cryptography provided in support of the secure administration.

**Table 5: SSHv2 Related Cryptography**

| Cryptographic Method | Use within SSHv2 |
|---|---|
| SP 800-56 Key Exchange | Used in SSHv2 session establishment. |
| RSA Digital Signatures | Used in SSHv2 session establishment. |
| ANSI X9.31 PRNG | Used in SSHv2 session establishment. |
| SHS | Used to provide SSHv2 traffic integrity verification. |

| | |
|---|---|
| AES | Used to encrypt SSHv2 session traffic. |

NOTE: See the entries for FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM_(EXT).2, FCS_CKM.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), and FCS_COP_(EXT).1 within section 6.1, "TOE Security Functional Requirement Measures" for additional details regarding the use of cryptography within SSHv2.

In support of the provided cryptography, the TOE performs a number of self-tests to ensure the correct operation. These tests include,

- Self tests to demonstrate the correct operation of the following cryptographic functions:
    - Key error detection;
    - cryptographic algorithms;
    - RNG/PRNG
- Self tests to demonstrate the correct operation of each key generation component
- Self tests to verify the integrity of TSF data related to the key generation
- Self tests to verify the integrity of stored TSF executable code
- Self tests to demonstrate the correct operation of the TSF

### 4.1.6 Security Audit

The ASR provides extensive auditing capabilities. The TOE can audit events related to security alarms, cryptographic functionality, information flow control enforcement, identification and authentication, and administrative actions. The ASR generates an audit record for each auditable event. In addition to generating audit records for auditable events, the TOE monitors the occurrences and identifies potential security violation based on the generated audit records. Once the ASR has detected a potential security violation, an alarm is generated and a message is displayed to administrators. Additionally, the Security Administrator can configure the TOE to generate an audible alarm to indicate a potential security violation and enforces confirmation of each alarm by an administrator. The ASR provides the Audit Administrator with a sorting and searching capability to improve audit analysis. The Security Administrator configures auditable events, backs-up and manages audit data storage. The TOE provides the Security Administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail.

### 4.1.7 High Availability

For ASR configurations that include dual ESPs or RPs, one of the ESPs or RPs act as the active hardware while the other acts as a hot standby. If there is a hardware failure within either the active ESP or active RP, the hot standby ESP or RP within the ASR automatically becomes active. If there is a software failure within the active software instance, the ASR automatically switches to the hot standby software instance resident within the TOE on the hot standby.

# 5 Assumptions

The following assumptions were made during the evaluation of Cisco Aggregation Services Router (ASR) 1000 Series:

- 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.
- Network resources shall be available to allow clients to satisfy mission requirements and to transmit information.

# 6 Documentation

The following documentation was used as evidence for the evaluation of the Cisco Aggregation Services Router (ASR) 1000 Series:

## 6.1 Design Documentation

1. Aggregation Services Router (ASR) 1000 Series Security Architecture Specification, Version 0.4, September, 2010
2. Aggregation Services Router (ASR) 1000 Series Functional Specification, Version 0.8, April 1, 2011
3. Aggregation Services Router (ASR) 1000 Series TOE Design Specification, Version 0.13, April 27, 2010
4. Aggregation Services Router (ASR) 1000 Series Functional Specification Annex B RFC Security Parameter Relevancy, Version 0.3, June 25, 2010
5. FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASR 1002f, ASR 1002 with ESP5 or ESP10, ASR 1004 with RP 1 or RP 2 and ESP10 or ESP20, and ASR 1006 with dual RP 1 or RP 2 and dual ESP10 or ESP20, firmware version: 2.4.2t

## 6.2 Guidance Documentation

1. Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance and Preparative Procedures, Version 0.7, April 2011
2. Cisco IOS Security Command Reference, April 2010
3. Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide, February 26, 2010 ( Text Part Number: OL-16506-06)
4. Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Software Configuration Guide, February 26, 2010 (Text Part Number: OL-14127-06)

5. Cisco ASR 1000 Series Aggregation Services Routers SIP and SPA Hardware Installation Guide, February 26, 2010 (Text Part Number: OL-14126-06)
6. Cisco ASR 1000 Series Aggregation Services Routers Hardware Installation and Initial Configuration Guide, November 2009 (Text Part Number: OL-13208-06)
7. Cisco ASR 1000 Series Shared Port Adapter Support
8. Cisco ASR 1000 Series Aggregation Services Routers Operations and Maintenance Guide, Text Part Number: OL-17665-03, June, 2009
9. Cisco IOS IP Routing: BGP Command Reference, November 2009
10. Cisco IOS IP Routing: ISIS Command Reference, November 2009
11. Cisco IOS IP Routing: OSPF Command Reference, November 2009
12. Cisco IOS IP Routing: RIP Command Reference, November 2009

*13*. Cisco IOS XE Network Management Configuration Guide, Release 2

## 6.3 Life Cycle

1. Configuration Management, Lifecycle and Delivery Procedures for Cisco Aggregation Services Router (ASR) 1000 Series IOS XE 4.2, ASR1K-CMP-v1-4, April 2011, Version: 1.4

## 6.4 Testing

1. ASR 1000 Series Common Criteria Test Documentation, Version 1.2, April 1, 2011
2. ASR1000 Series Router Test Guidance for Common Criteria Certification, EDCS-773245, April 29, 2011
3. ASR1000 Series Router Test Guidance – for Common Criteria Certification – Part 2, EDCS-971972, April 27, 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 Aggregation Services Router (ASR) 1000 Series, Version 2.0, May 11, 2011.

## 7.1 Developer Testing

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

1. Identification & Authentication
2. Security Management
3. VPN, Router, and/or Firewall Information Flow Control
4. Trusted Channel/Path

5. Cryptography
6. Security Audit

## 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 the Cisco Aggregation Services Router (ASR) 1000 Series including:

- ASR 1002f, ASR 1002, ASR 1004, ASR 1006 running IOS XE 2.4.2t

To use the product in the evaluated configuration, the product must be configured as specified in the **Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance and Preparative Procedures, Version 0.7, April 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 EAL4 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 4) augmented with ALC_FLR.2 requirements.

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

## 9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit.  The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Aggregation Services Router (ASR) 1000 Series product that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.2 Evaluation of the Development (ADV)

The evaluation team applied each EAL 4 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification and a detailed design document. The evaluation team also ensured that the correspondence analysis between the design abstractions correctly demonstrated that the lower abstraction was a correct and complete representation of the higher abstraction.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each EAL 4 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. Both of these guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.4 Evaluation of the Life Cycle Support Activities (ALC)

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

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

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

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

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.6 Vulnerability Assessment Activity (VAN)

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

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

## 9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's performance of the entire vendor tests suite, the independent tests, and the penetration test also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

# 10 Validator Comments/Recommendations

The validation team considers the evaluated subset of product functions to be consistent with the product's intended purpose and mode of operation. The rationale for excluded features is plausible and introduces no unreasonable constraints.

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

Although the vendor apparently maintains a significant internal organization responsible for vulnerability analysis and flaw remediation, the evaluation team was not provided access to any of that organization's personnel nor to the vulnerability reports and analysis performed therein. Again, while the materials provided are sufficient to satisfy the conformance requirements for vulnerability analysis and flaw remediation, the validation team considers the lack of access a lost opportunity to assess and describe the details of analysis and remediation work performed by the vendor.

While the TOE implements FPT_FLS, the scope of applicability of this requirement is limited to the functions of the cryptomodule. While the TOE provides other reliability and availability features and can be used in configurations that offer enhanced resilience to failures, these mechanisms and configurations were not tested as part of the evaluation process.

# 11 Annexes

Not applicable.

# 12 Security Target

The Security Target is identified as *Cisco Aggregation Services Router (ASR) 1000 Series Security Target Security Target, Version 0.19, 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 Aggregation Services Router (ASR) 1000 Series Part 2 (Proprietary)*, Version 2.0, May 11, 2011.

[7] Science Applications International Corporation. *Evaluation Team Test Report for the Cisco Aggregation Services Router (ASR) 1000 Series, ETR Part 2 Supplement (SAIC and Cisco Proprietary)*, Version 2.0, May 11, 2011.

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

[10] Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version 0.19, May 2011.