National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Cisco Aggregation Services Router (ASR) 1000 Series

Report Number: CCEVS-VR-VID10518-2013
Version 1.0
December 19, 2013

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

Jerome Myers, Ph.D., Senior Validator
The Aerospace Corporation

Patrick Mallett, Ph.D. Lead Validator
The MITRE Corporation

Common Criteria Testing Laboratory

Chris Gugel, CC Technical Director
Justin Fisher
Josh Jones
John Schroeder
Jeremy Sestok

Booz Allen Hamilton (BAH)
Linthicum Heights, 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, 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 Booz Allen Hamilton Inc. Common Criteria Testing Laboratory (CCTL) in Linthicum Heights, Maryland, United States of America, and was completed in December 2013. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Booz Allen. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements set forth in the Network Device Protection Profile (NDPP).

The Target of Evaluation (TOE) is the Cisco Aggregation Services Router (ASR) 1000 Series, with software image Release 3.7.2t(S). The Cisco ASR 1000 Series TOE is a purpose-built, routing platform. The TOE delivers embedded hardware acceleration for multiple Cisco IOS® XE Software services.

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 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4), as interpreted by the Assurance Activities contained in the NDPP. 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 is consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes, and reviewed the individual work units of the ETR for the NDPP Assurance Activities. 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 technical information included in this report was obtained from the Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version .15, December 2013 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). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

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 Product Compliance 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 Aggregation Services Router (ASR) 1000 Series, with software image Release 3.7.2t(S) *Refer to Table 2 for Hardware Models and Specifications
Protection Profile	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional IPSec requirements)
Security Target	Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version .15, December 2013
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation "Cisco Aggregation Services Router (ASR) 1000 Series" Evaluation Technical Report v3.0 dated December 3 2013
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Booz Allen Hamilton, Linthicum, Maryland
CCEVS Validators	Jerome Myers, Ph.D, The Aerospace Corporation Patrick Mallett, Ph.D. The MITRE Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

The following lists the threats addressed by the TOE. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

- **T.ADMIN_ERROR** — An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.UNDETECTED_ACTIONS** — Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
- **T.UNAUTHORIZED_ACCESS** — A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
- **T.UNAUTHORIZED_UPDATE** — A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
- **T.USER_DATA_REUSE** — User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Objectives

The following identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies identified.

- **O.PROTECTED_COMMUNICATIONS —** The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
- **O.VERIFIABLE_UPDATES —** The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
- **O.SYSTEM_MONITORING —** The TOE will provide the capability to generate audit data and send those data to an external IT entity.
- **O.DISPLAY_BANNER —** The TOE will display an advisory warning regarding use of the TOE.
- **O.TOE_ADMINISTRATION —** The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
- **O.RESIDUAL_INFORMATION_CLEARING —** The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
- **O.SESSION_LOCK —** The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
- **O.TSF_SELF_TEST —** The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly**.**

3.4 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Security Requirements for Network Devices, Version 1.1, 08 June 2012 (including the optional IPSec requirements) to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

The TOE includes all the code that enforces the policies identified (see Section 5).

The evaluated configuration of the TOE includes the Cisco Aggregation Services Router (ASR) 1000 Series, with software image Release 3.7.2t(S) product that is comprised of one or more of the product models.

The Non-FIPS 140-2 mode of operation is excluded from the evaluation. This mode will be disabled by configuration. The exclusion of this functionality does not affect compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1.

4 Architectural Information

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

4.1 TOE Introduction

The Target of Evaluation (TOE) is the Cisco Aggregation Services Router (ASR) 1000 Series. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

The TOE consists of one or more models as specified in Section 3.2 below and includes the Cisco IOS-XE software image Release 3.7.2t(S). The TOE's hardware is modular, consisting of four components:

- Chassis: The TOE chassis includes 1-RU, 2-RU, 4-RU, 6-RU and 13-RU form factors. The chassis is the component of the TOE in which all other TOE components are housed.
- Embedded Services Processor (ESPr): The Cisco ASR 1000 Series ESPrs 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.

4.2 Physical Boundaries

The TOE is a hardware and software solution that is made up of the following router models: ASR 1001, ASR 1002, ASR 1002X, ASR 1004, ASR 1006, and ASR 1013. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 3.7.2t(S). The TOE's physical boundary is one or more models with the hardware specifications defined within Table 2 below.

Table 2 – Hardware Models and Specifications

Hardware Model	ASR 1001	ASR 1002-X	ASR 1002	ASR 1004	ASR 1006	ASR 1013
Chassis Size	1-Rack Unit	2-Rack Units	2-Rack Units	4-Rack Units	6-Rack Units	13-Rack Units
Power	DC power: 500W AC Power: 471W	DC power: 590W AC Power: 560W	DC power: 590W AC Power: 560W	DC power: 1020W AC Power: 960W	DC power: 1700W AC Power: 1600W	DC power: 4000W AC Power: 3760W

Supported ESPrs	Integrated ESP	Integrated ESP	ESP5 ESP10	ESP10 ESP20	Dual ESP10 Dual ESP20 Dual ESP40 Dual ESP100	Dual ESP40 Dual ESP100
Supported RPs	Integrated RP1	Integrated RP1	Integrated RP1	RP1 RP2	Dual RP1 Dual RP2	Dual RP2
SPA Slots	1 SPA slot	1 SPA slot	3 SPA slots	8 SPA slots	12 SPA slots	24 SPA slots
Supported SPAs	Cisco 1-Port Clear Channel OC3 ATM Shared Port Adapter (SPA-1XOC3-ATM-V2) Cisco 3-Port Clear Channel OC3 ATM Shared Port Adapter (SPA-3XOC3-ATM-V2) Cisco 1-Port OC12 STM Shared Port Adapter (SPA-1XOC12-ATM-V2) Cisco 2-Port T3/E3 Circuit Emulation and ATM SPA (SPA-2CHT3-CE-ATM) Cisco 8-Port Channelized T1/E1 Shared Port Adapter (SPA-8XCHT1/E1) Cisco 4-Port Channelized T3 (DS0) Shared Port Adapter (SPA-4XCT3/DS0) Cisco 2-Port Channelized T3 (DS0) Shared Port Adapter (SPA-2XCT3/DS0) Cisco 1-port Channelized STM-1/OC-3c to DS0 Shared Port Adapter (SPA-1XCHSTM1/OC3) Cisco 2-Port Clear Channel T3/E3 Shared Port Adapter (SPA-2XT3/E3) Cisco 4-Port Clear Channel T3/E3 Shared Port Adapter (SPA-4XT3/E3) Cisco 4-Port Serial Interface Shared Port Adapter (SPA-4XT-Serial) 1-port Channelized OC12 to DS0 SPA (SPA-1XCHOC12/DS0) Cisco 4-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-4X1FE-TX-V2) Cisco 8-Port 10BASE-T/100BASE Fast Ethernet Shared Port Adapter (SPA-8X1FE-TX-V2) Cisco 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE-V2) Cisco 5-Port Gigabit Ethernet Shared Port Adapter (SPA-5X1GE-V2) Cisco 8-Port Gigabit Ethernet Shared Port Adapter (SPA-8X1GE-V2) Cisco 10-Port Gigabit Ethernet Shared Port Adapter (SPA-10X1GE-V2) Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter (SPA-1X10GE-L-V2) Cisco 1-port 10GE LAN/WAN-PHY Shared Port Adapter (SPA-1X10GE-WL-V2) Cisco Synchronous Ethernet SPA (SPA-2X1GE-SYNCE) Cisco 2-Port OC3c/STM-1c POS Shared Port Adapter (SPA-2XOC3-POS) Cisco 4-Port OC3c/STM-1c POS Shared Port Adapter (SPA-4XOC3-POS) Cisco 8-port OC3/STM4 POS Shared Port Adapter (SPA-8XOC3-POS) Cisco 1-Port OC12c/STM-4c POS Shared Port Adapter (SPA-1XOC12-POS) Cisco 2-port OC12/STM4 POS Shared Port Adapter (SPA-2XOC12-POS) Cisco 4-port OC12/STM4 POS Shared Port Adapter (SPA-4XOC12-POS) Cisco 8-port OC12/STM4 POS SPA Shared Port Adapter (SPA-8XOC12-POS) Cisco 1-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-1XOC48-POS/RPR) Cisco 2-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-2XOC48POS/RPR) Cisco 4-port OC48/STM16 POS/RPR Shared Port Adapter (SPA-4XOC48POS/RPR) Cisco 1-Port OC-192c/STM-64c POS/RPR Shared Port Adapter with XFP Optics (SPA-OC192POS-XFP)						
Interfaces	Port Adapter Interface Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface (3) Console Port Auxiliary Port 10/100 BITS Ethernet Port 10/100 Management Ethernet Port USB Port GigE Ports (4)	Port Adapter Interface (8) Console Port Auxiliary Port 10/100 Management Ethernet Port 10/100 BITS Ethernet Port (1) USB Ports (2)	Port Adapter Interface (12) Console Port Auxiliary Port (2) 10/100 BITS Ethernet Port (2) 10/100 Management Ethernet Port (2) USB Ports (4)	Port Adapter Interface (24) Console Port Auxiliary Port (2) 10/100 BITS Ethernet Port (4) 10/100 Management Ethernet Port (4) USB Ports (4)

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

Table 3 – IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS or TACACS+ AAA Server	No	This includes any IT environment RADIUS or TACACS+ AAA server that can be leveraged for remote user authentication.
Management Workstation	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration through protected channels. This management workstation must have an IPsec connection established between itself and the managed instance of ASR1K. This connection will be used to protect a tunneled protocol that will be used for user authentication and to perform ASR1K management actions. While the tunneled protocol used through IPsec is not defined by the ST and can be either SSH or telnet, it is recommended to use SSHv2.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
NTP Server	No	The TOE supports communications with an NTP server. A solution must be used that supports MD5 hashing of communications with up to a 32 character key.

5 Security Policy

5.1 Security Audit

The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail or a configurable audit trail threshold to track the storage capacity of the audit trail. Audit logs are backed up over an encrypted channel to an external audit server.

5.2 Cryptographic Support

The TOE provides cryptography in support of ASR 1000 Series security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 (see Table 6 for certificate references).

Table 4 – FIPS References

Algorithm	Supported Mode	Cert. #
AES	CBC (128, 192, 256) ECB, CBC (128, 192, 256)	333, 2346, 2549
SHS	Byte Oriented	408, 2023, 2150
HMAC	Byte Oriented	137, 1455, 1570
RNG (ANSI X9.31)	Triple-DES (EDE)	154
Triple-DES	KO 1, CBC	397, 1170, 1469, 1543
DRBG	CTR (using AES-256)	382
RSA	PKCS#1 v.1.5, 1024-4096 bit key, FIPS 186-2 Key Gen	1304

The TOE provides cryptography in support of secure connections with other IT entities via IPSec. All keys are zeroized when no longer needed. The cryptographic services provided by the TOE include are described in the table below.

Table 5 – TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPSec session.
RSA Signature Services	Used in IPSec session establishment.
SP 800-90 RBG	Used in IPSec session establishment.
SHS	Used to provide IPSec traffic integrity verification
AES	Used to encrypt IPSec session traffic.

5.3 User Data Protection

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

5.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of remote IT device peers and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPSec mutual authentication.

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrative interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or remote interfaces. The TOE optionally supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE’s CLI.

5.5 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 IPSec session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users; all identification and authentication; all audit functionality of the TOE; all TOE cryptographic functionality; the timestamps maintained by the TOE; updates to the TOE; and TOE configuration file storage and retrieval. The TOE supports two separate administrative roles: non-privileged Administrator and privileged Administrator. Only the privileged administrator can perform all of the above security relevant management functions. The privileged Administrator is also considered to be the Authorized Administrator.

5.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE’s clock manually, or can configure the TOE to use NTP to synchronize the TOE’s clock with an external time source. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of malicious software.

5.7 TOE Access

The TOE can terminate or lock inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the “exit” command.

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

5.8 Trusted Path/Channels

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 IPSec secure connection.

The TOE establishes a trusted channel between itself and peer IT devices, syslog servers, RADIUS Servers, and TACACS+ Servers. This trusted channel is secured via IPSec encryption.

6 Documentation

The vendor provides guidance documentation on their support website, http://www.cisco.com/web/strategy/government/security_certification/net_business_benefit_seccert_common_criteria.html. The following documentation located on their support website was used as evidence for the evaluation of the Cisco Aggregation Services Router (ASR) 1000 Series:

- *Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures version .13*

There are many documents available on the support website, but the above mentioned document is the only one that is to be trusted as having been part of the evaluation. This guidance document contains the security-related guidance material for this evaluation and must be referenced to place the product within the Common Criteria evaluated configuration. The guidance document is applicable for all models of the ASR 1000 Series product claimed by this evaluation. Additionally, the guidance document contains references and pointers to other TOE guidance documentation for additional detail regarding the security-related functionality. These references were also examined during the evaluation.

7 Evaluated Configuration

The evaluated configuration, as defined in the Security Target, is one or more Cisco Aggregation Services Router (ASR) 1000 Series running the Cisco IOS-XE software image Release 3.7.2t(S). This includes the ASR 1000 Series models ASR 1001, ASR 1002, ASR 1002X, ASR 1004, ASR 1006, and ASR 1013, and their associated modular components defined in Table 2.

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 .13* document. Refer to Section 7 for information on where to retrieve the document from Cisco's support website and how to use this document to configure the TOE into the evaluated configuration.

8 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 Technical Report for a Target of Evaluation "Cisco Aggregation Services Router (ASR) 1000 Series" Evaluation Technical Report v3.0 dated December 3 2013*, which is not publically available.

8.1 Test Configuration

The evaluation team configured each model of the TOE according the *Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures version .13* document for testing.

The following environment components and test tools* were utilized during the testing:

- RADIUS Server: freeradius 2.1.10+dfsg-3ubuntu0.12.04.1
- TACACS+ Sever: tacacs+ 4.0.4.19-11build1
- Syslog Server: rsyslog 5.8.6-1ubuntu8.1 (note: this is an extension to sysklogd 1.5-6ubuntu1)
- NTP Server: ntp_4.2.6.p3+dfsg-1ubuntu3.1_i386
- Putty client: version .60
- WireShark: version 1.10.0

*Only the test tools utilized for functional testing have been listed.

The following three figures depict the configurations for the test environment that were utilized during the execution of the testing:

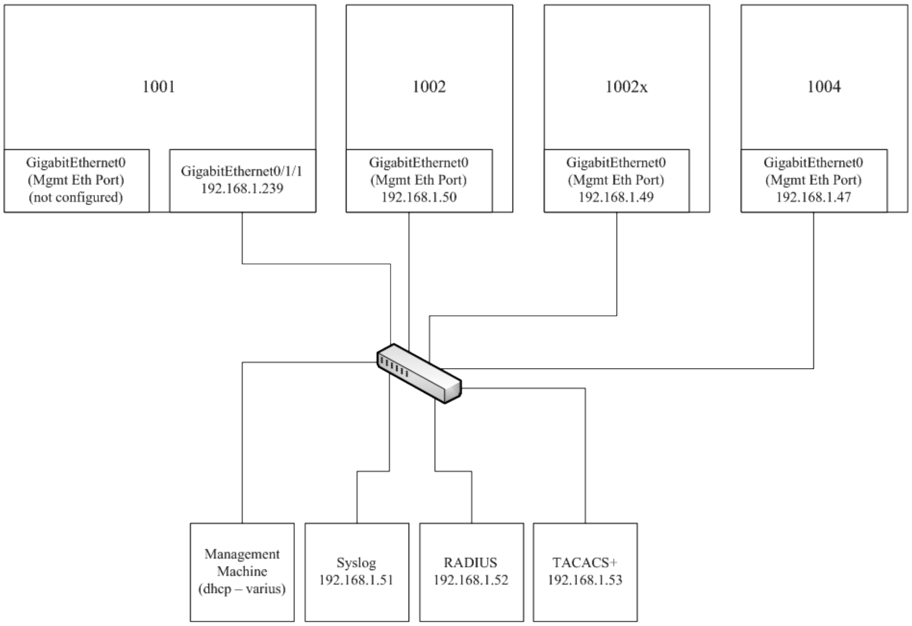
1001
GigabitEthernet0 (Mgmt Eth Port) (not configured)
GigabitEthernet0/1/1 192.168.1.239
1002
GigabitEthernet0 (Mgmt Eth Port) 192.168.1.50
1002x
GigabitEthernet0 (Mgmt Eth Port) 192.168.1.49
1004
GigabitEthernet0 (Mgmt Eth Port) 192.168.1.47
Management Machine (dhcp – varius)
Syslog 192.168.1.51
RADIUS 192.168.1.52
TACACS+ 192.168.1.53

Figure 1

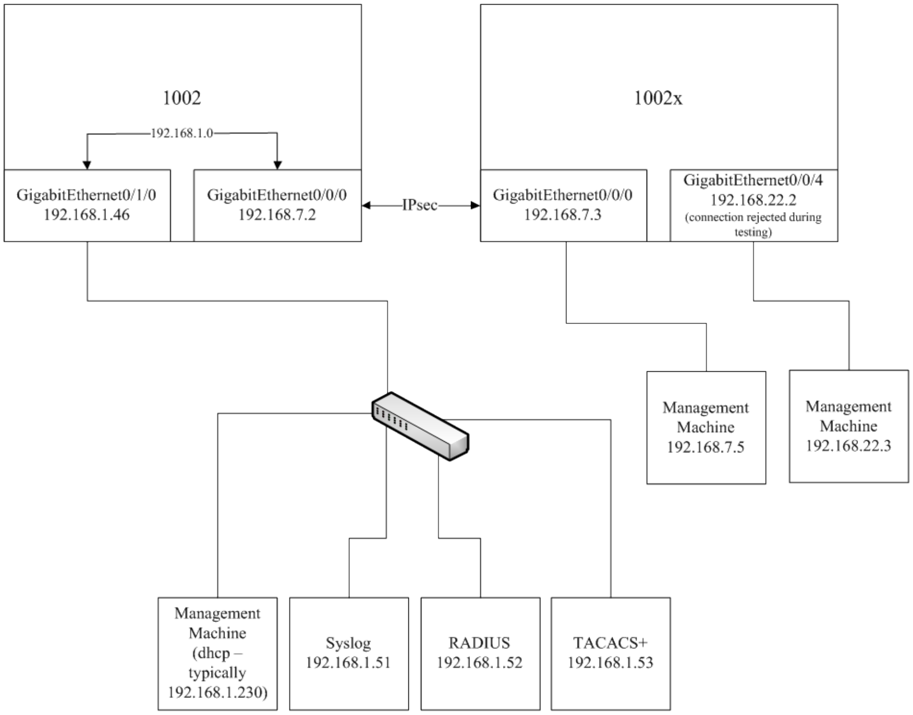

Figure 2

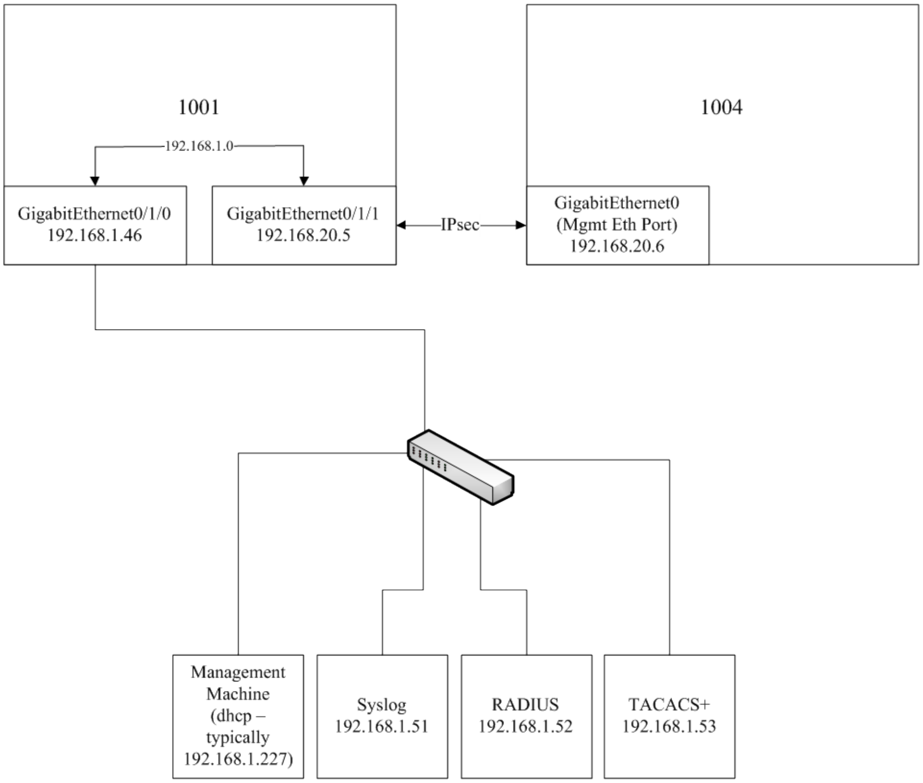

Figure 3

8.2 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.3 Evaluation Team Independent Testing

The test team's test approach was to test the security mechanisms of Cisco Aggregation Services Router (ASR) 1000 Series by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, Functional Specification (FSP), and the independent test plan were used to demonstrate test coverage of all Assurance Activities defined within the *Security Requirements for Network Devices, Version 1.1, 08 June 2012* (including the optional IPSec requirements) Protection Profile for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

- change the security state of the product,
- permit an object access or information flow that is regulated by the security policy,
- are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface. The evaluation team tested each interface for all relevant behavior of the TOE that applied to that interface.

The table below describes the test configuration(s) utilized when performing the NDPP’s Test Assurance Activities for the specified requirement

Security Functional Requirement	Test Configuration(s)
FAU_GEN.1	Figures 1, 2 and 3
FAU_GEN.2	Figures 1, 2 and 3
FAU_STG_EXT.1	Figures 2 and 3
FCS_CKM.1	Figure 1
FCS_COP.1(1)	Figure 1
FCS_COP.1(2)	Figure 1
FCS_COP.1(3)	Figure 1
FCS_COP.1(4)	Figure 1
FCS_RBG_EXT.1	Figure 1
FCS_IPSEC_EXT.1	Figures 2 and 3
FIA_PMG_EXT.1	Figure 1
FIA_UIA_EXT.1	Figure 1
FIA_UAU_EXT.2	Figure 1
FIA_UAU.7	Figure 1
FPT_STM.1	Figure 1
FPT_TUD_EXT.1	Figure 1
FTA_SSL_EXT.1	Figure 1
FTA_SSL.3	Figure 1
FTA_SSL.4	Figure 1
FTA_TAB.1	Figure 1
FTP_ITC.1	Figures 2 and 3
FTP_TRP.1	Figures 2 and 3

8.4 Evaluation Team Vulnerability Testing

The evaluation team created a set of vulnerability tests to attempt to subvert the security of the TOE. These tests were created based upon the evaluation team's review of the vulnerability analysis evidence and independent research. The evaluation team conducted searches for public vulnerabilities related to the TOE. A few notable resources consulted include securityfocus.com, the cve.mitre.org, and the nvd.nist.gov.

Upon the completion of the vulnerability analysis research, the team had identified several generic vulnerabilities upon which to build a test suite. These tests were created specifically with the intent of exploiting these vulnerabilities within the TOE or its configuration. All three test configurations were utilized during the vulnerability testing.

The team tested the following areas:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network.
- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.
- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

  Backdoors
  CGI abuses
  Denial of Service
  Finger abuses
  Firewalls
  FTP
  Gain a shell remotely
  Gain root remotely
  General
  Miscellaneous
  Netware
  NIS
  Port scanners
  Remote file access
  RPC
  Settings
  SMTP Problems
  SNMP
  Untested
  Useless services

- Malformed Packet Flooding
  This attack attempts to exercise the stability of the IP stack and its components by sending a large amount of TCP packets and malformed TCP packets in an attempt to overload the application. If successful, the TOE will crash and not allow any connections until the TOE is rebooted.
- Management Network Denial of Service (DoS)
  This attack attempts to utilize proof of concept code to perform a denial of service attack against OpenSSH and the FTP functionality used in the TOE. A successful attack will deny service to FTP or other management functionality in the TOE.
- CLI Privilege Escalation
  This attack attempts to break out of the custom CLI and access the underlying Linux command line.
- VLAN Hopping
  In this test, the attacker attempts to jump from one VLAN to another on a network device.

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 Assurance Activities and 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 4 and CEM version 3.1 rev 4. The evaluation determined the Cisco Aggregation Services Router (ASR) 1000 Series TOE to be Part 2 extended, and meets the SARs contained the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

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. Additionally the evaluator performed an assessment of the Assurance Activities specified in the Security Requirements for Network Devices Protection Profile (NDPP).

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 1 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 contained in the Security Target's TOE Summary Specification as well as a separately developed Functional Specification document. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the TOE Summary Specification.

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 Assurance Activities, 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 1 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. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the NDPP related to the examination of the information contained in the operational guidance documents.

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 Assurance Activities, 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 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

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 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and recorded the results in a Test Report, summarized in the Evaluation Technical Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the NDPP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with 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 addressed the vulnerability analysis Assurance Activities in the NDPP, 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 test activities 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 performed the Assurance Activities in the NDPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments

The CCTL did not explicitly test in a configuration which had an encrypted communications channel all the way from the TOE to an audit server. The user guide was updated to indicate that an IPsec connection can be directly to a client on the server or physically connected to a ASR1K product as long as any connections that leave that subnet are protected via IPsec.

The CCTL did not test all possible configurations of TOE component platforms. However, the lab provided an excellent equivalency argument for covering testing of the multitude of platforms.

11 Annexes

Not applicable

12 Security Target

The security target for this product's evaluation is *Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version .15, December 2013*.

13 List of Acronyms

Acronym	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
EAL	Evaluation Assurance Level
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
ESPr	Embedded Services Processors
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
ISDN	Integrated Services Digital Network
IT	Information Technology
NDPP	Network Device Protection Profile
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
ST	Security Target
TCP	Transport Control Protocol
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network
WIC	WAN Interface Card

14 Terminology

Terminology	Definition
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer	Another router on the network that the TOE interfaces with.
Privilege level	Assigns a user specific management access to the TOE to run specific commands. The privilege levels are from 1-15 with 15 having full administrator access to the TOE similar to root access in UNIX or Administrator access on Windows. Privilege level 1 has the most limited access to the CLI. By default when a user logs in to the Cisco IOS, they will be in user EXEC mode (level 1). From this mode, the administrator has access to some information about the TOE, such as the status of interfaces, and the administrator can view routes in the routing table. However, the administrator can't make any changes or view the running configuration file. The privilege levels are customizable so that an Authorized Administrator can also assign certain commands to certain privilege levels.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another router.
Role	An assigned role gives a user varying access to the management of the TOE. For the purposes of this evaluation the privilege level of user is synonymous with the assigned privilege level.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vty	Is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). For configuration purposes vty defines the line for remote access policies to the router.

15 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version .15, December 2013.
6. Evaluation Technical Report for a Target of Evaluation "Cisco Aggregation Services Router (ASR) 1000 Series" Evaluation Technical Report v3.0 dated December 3 2013.
7. *Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures version .13*