

National Information Assurance Partnership



Common Criteria Evaluation and Validation Scheme Validation Report

Cisco Aggregation Services Router (ASR) 1000 Series

Report Number: CCEVS-VR-VID10609-2015
Version 1.0
June 11, 2015

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

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers, Senior Validator
The Aerospace Corporation

Luke Florer, Lead Validator
The Aerospace Corporation

Common Criteria Testing Laboratory

Chris Gugel, CC Technical Director
Dave Cornwell
Justin Fisher
Kevin Le
Chris Rakaczky

Booz Allen Hamilton (BAH)
Linthicum Heights, Maryland

Table of Contents

1	EXECUTIVE SUMMARY	4
2	IDENTIFICATION	6
3	ASSUMPTIONS AND CLARIFICATION OF SCOPE	7
4	ARCHITECTURAL INFORMATION	10
4.1	TOE INTRODUCTION	10
4.2	PHYSICAL BOUNDARIES	10
5	SECURITY POLICY	12
5.1	SECURITY AUDIT	12
5.2	CRYPTOGRAPHIC SUPPORT.....	12
5.3	USER DATA PROTECTION.....	13
5.4	IDENTIFICATION AND AUTHENTICATION	13
5.5	SECURITY MANAGEMENT	14
5.6	PACKET FILTERING	14
5.7	PROTECTION OF THE TSF.....	14
5.8	TOE ACCESS.....	15
5.9	TRUSTED PATH/CHANNELS.....	15
6	DOCUMENTATION	16
7	EVALUATED CONFIGURATION	17
8	IT PRODUCT TESTING	18
8.1	TEST CONFIGURATION	18
8.2	DEVELOPER TESTING	18
8.3	EVALUATION TEAM INDEPENDENT TESTING.....	18
8.4	EVALUATION TEAM VULNERABILITY TESTING.....	19
9	RESULTS OF THE EVALUATION	20
9.1	EVALUATION OF THE SECURITY TARGET (ASE)	20
9.2	EVALUATION OF THE DEVELOPMENT (ADV).....	20
9.3	EVALUATION OF THE GUIDANCE DOCUMENTS (AGD).....	20
9.4	EVALUATION OF THE LIFE CYCLE SUPPORT ACTIVITIES (ALC).....	21
9.5	EVALUATION OF THE TEST DOCUMENTATION AND THE TEST ACTIVITY (ATE).....	21
9.6	VULNERABILITY ASSESSMENT ACTIVITY (VAN)	21
9.7	SUMMARY OF EVALUATION RESULTS	21
10	VALIDATOR COMMENTS	23
11	ANNEXES	24
12	SECURITY TARGET	25
13	LIST OF ACRONYMS	26
14	TERMINOLOGY	27
15	BIBLIOGRAPHY	28

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 June 2015. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports. 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) and VPN Gateway Extended Package (VPN GW EP).

The Target of Evaluation (TOE) is the Cisco Aggregation Services Router (ASR) 1000 Series, with software version IOS XE 3.13. The Cisco ASR 1000 Series 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 provides IPsec connection capabilities to facilitate secure communications with external entities, as required.

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 and VPN GW EP. 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, reviewed the individual work units of the ETR, and the Assurance Activities Report (AAR) for the NDPP and VPN GW EP 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.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

The technical information included in this report was obtained from the Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version 0.4, May 5, 2015 and analysis performed by the Validation Team.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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(s) 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 version IOS XE 3.13 *Refer to Table 2 for Models and Specifications
Protection Profile	Protection Profile for Network Devices, Version 1.1, 08 June 2012 (including the optional IPsec and SSH requirements) and Errata #2; Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013
Security Target	Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version 0.4, May 5, 2015
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation “Cisco Aggregation Services Router (ASR) 1000 Series” Evaluation Technical Report v1.0 dated April 1, 2015
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, The Aerospace Corporation Luke Florer, The Aerospace 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.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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.
- **T.NETWORK_DISCLOSURE** — sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
- **T.NETWORK_ACCESS** — unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network.
- **T.NETWORK_MISUSE** — access to services made available by a protected network might be used counter to Operational Environment policies.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

- **T.TSF_FAILURE** — Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
- **T.REPLAY_ATTACK** — if malicious or external IT entities are able to gain access to the network, they may have the ability to capture information traversing throughout the network and send them on to the intended receiver.
- **T.DATA_INTEGRITY** — a malicious party attempts to change the data being sent – resulting in loss of integrity.

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.
- **O.ADDRESS_FILTERING** — the TOE will provide the means to filter and log network packets based on source and destination addresses.
- **O.AUTHENTICATION** — the TOE will provide a means to authenticate the user to ensure they are communicating with an authorized external IT entity.
- **O.CRYPTOGRAPHIC_FUNCTIONS** — the TOE will provide means to encrypt and decrypt data as a means to maintain confidentiality and allow for detection and modification of TSF data that is transmitted outside of the TOE.
- **O.FAIL_SECURE** — upon a self-test failure, the TOE will shutdown to ensure data cannot be passed while not adhering to the security policies configured by the administrator.
- **O.PORT_FILTERING** — the TOE will provide the means to filter and log network packets based on source and destination transport layer ports.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 Protection Profile for Network Devices, Version 1.1, 08 June 2012 (including the optional IPsec and SSH requirements) with Errata #2, and Network Device Protection Profile (NDPP) Extended Package VPN Gateway, Version 1.1, 12 April 2013 to which this evaluation claimed exact compliance.
- Consistent with the expectations of the Protection Profiles, 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 evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation

The evaluated configuration of the TOE includes the Cisco Aggregation Services Router (ASR) 1000 Series, with software version IOS XE 3.13 product that is comprised of one or more of the product models. The TOE includes all the code that enforces the policies identified (see Section 5).

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 either the Protection Profile for Network Devices Version 1.1 or the Network Device Protection Profile (NDPP) Extended Package VPN Gateway 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 Cisco ASR 1000 Series 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 provides IPSec connection capabilities to facilitate secure communications with external entities, as required. The TOE consists of one or more models as specified in Section 4.2 below and includes the software version IOS XE 3.13.

4.2 Physical Boundaries

The TOE is a hardware and software solution that makes up the router models as follows: Chassis: ASR1001X, ASR 1002X, ASR 1006, ASR 1013; Embedded Services Processors (ESP): ESP100, ESP200; Route Processor (RP): RP2. The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 3.13. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE is comprised of the following physical specifications as described in the table below:

Table 2 – Hardware Models and Specifications

Hardware Model	ASR 1001-X	ASR 1002-X	ASR 1006	ASR 1013
Size	1-Rack Unit	2-Rack Units	6-Rack Units	13-Rack Units
Power	DC power: 500W AC Power: 471W	DC power: 590W AC Power: 560W	DC power: 1700W AC Power: 1600W	DC power: 4000W AC Power: 3760W
Supported ESPs	Integrated ESP	Integrated ESP	Dual ESP100	Dual ESP100 ESP200
Supported RPs	Integrated RP	Integrated RP	Dual RP2	Dual RP2
SPA Slots	1 SPA slot	1 SPA slot	12 SPA slots	24 SPA slots

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

Interfaces	<ul style="list-style-type: none"> • Port Adapter Interface • Console Port • Auxiliary Port • 10/100 BITS Ethernet Port • 10/100 Management Ethernet Port • USB Port • GigE Ports (4) 	<ul style="list-style-type: none"> • Port Adapter Interface • Console Port • Auxiliary Port • 10/100 BITS Ethernet Port • 10/100 Management Ethernet Port • USB Port • GigE Ports (4) 	<ul style="list-style-type: none"> • Port Adapter Interface (12) • Console Port • Auxiliary Port (2) • 10/100 BITS Ethernet Port (2) • 10/100 Management Ethernet Port (2) • USB Ports (4) 	<ul style="list-style-type: none"> • 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 AAA Server	No	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
Remote VPN Gateway/Peer	Yes	This includes any VPN peer with which the TOE participates in VPN communications. Remote VPN Endpoints may be any device that supports IPsec VPN communications.
NTP Server	No	The TOE supports communications with an NTP server in order to synchronize the date and time on the TOE with the NTP server's date and time. A solution must be used that supports secure communications with up to a 32 character key.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.
Another instance of the TOE	No	Includes "another instance of the TOE" that would be installed in the evaluated configuration, and likely administered by the same personnel. Used as a VPN peer.

5 Security Policy

5.1 Security Audit

The Cisco ASR 1000 Series provide extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Aggregation Services Router (ASR) 1000 Series generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. 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 other Cisco ASR 1000 Series security functionality. This cryptography has been validated for conformance to the requirements of FIPS 140-2 Level 2 [Reference: CMVP Cert#2090] (see Table 4 for certificate references). The TOE utilizes the Intel Xeon hardware for this.

Table 4 FIPS References

Algorithm	Supported Mode	Cert. #
AES	CBC (128, 192, 256) ECB (128, 192, 256)	2817
SHS	Byte Oriented	2361, 2338
HMAC	Byte Oriented	1764
Triple-DES	KO 1, CBC	1670, 1671, 1688
DRBG	CTR (using AES-256)	481
RSA	PKCS#1 v.1.5, 1024-4096 bit key, FIPS 186-2 Key Gen	1471

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2. The cryptographic services provided by the TOE are described in Table 5 below.

Table 5 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA/DSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

Cryptographic Method	Use within the TOE
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services
ECC	Used to provide cryptographic signature services
DH	Used as the Key exchange method for SSH

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 zeroes. Residual data is never transmitted from the TOE.

5.4 Identification and Authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN 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 supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE optionally supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec, and SSH connections.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;
- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality;
- TOE configuration file storage and retrieval.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authenticated administrators.

Administrators can create configurable login banners to be displayed at time of login, and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

5.6 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers as well as between remote VPN clients and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

5.7 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. Additionally Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

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

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 unauthorized software.

Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

5.8 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.

5.9 Trusted Path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2, and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect communications with a CA or remote administrative console.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 ASR 1000 Series:

- *Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures, Version 0.4*

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 Cisco 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, with software version IOS XE 3.13.

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 0.4* document. Refer to Section 6 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 v1.0 dated April 1, 2015*, which is not publically available. The *Assurance Activities Report for a Target of Evaluation Cisco Aggregation Services Routers (ASR) 1000 Series, Version 1.0, dated May 5, 2015* provides an overview of testing and the prescribed assurance activities.

8.1 Test Configuration

The evaluation team configured each tested model of the TOE according the *Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures, Version 0.4* document for testing. The following TOE models (all claimed models) were tested:

- ASR 1001-X
- ASR 1002-X
- ASR 1006
- ASR 1013

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

- Syslog Server: rsyslog 5.8.6-1ubuntu8.1 (note: this is an extension to sysklogd 1.5-6ubuntu1) was used for testing
- NTP Server: ntp_4.2.6.p3+dfsg-1ubuntu3.1_i386
- RADIUS Server: freeradius 2.1.10+dfsg-3ubuntu0.12.04.1
- CA Server: Windows Server 2012 R2
- WireShark: version 1.12.1
- Bitwise SSH Client: version 4.60

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

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 the Cisco ASR 1000 Series by exercising the external interfaces to the TOE and viewing the TOE behavior on the platform. The ST, the vendor automated test cases and the independent test cases were used to demonstrate test coverage of all SFR testing assurance activities as defined by the NDPP and VPN GW EP for all *security relevant* TOE external interfaces. TOE external interfaces that will be 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,

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

- 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.

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.

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.
- **Malformed Packet Flooding**
This attack attempts to exercise the stability of the IP stack and its components by sending a large amount of TCP/UDP/ICMP/other IP packets and malformed TCP/UDP/ICMP/other IP packets in an attempt to overload the application. If successful, the TOE would have crashed and not allow any connections until the TOE was rebooted.
- **CLI Privilege Escalation**
This attack attempted to break out of the custom CLI and access the underlying Linux command line over SSH.
- **Undefined IP Protocol Packet Filtering**
In this test, the attacker attempted to generate network packets that cycle through all of the values for the Transport Layer Protocol attribute that are undefined by the RFCs for IPv4 and IPv6. Since none of these packets matched a rule, or belonged to an allowed session, the packets were dropped by the TOE.

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 documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The CCTL gave each Assurance Activity and work unit 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 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 Network Devices Protection Profile (NDPP) and VPN Gateway Extended Package (VPN GW EP).

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 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 NDPP and VPN GW EP.

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 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. Additionally the evaluator performed the Assurance Activities specified in the NDPP and VPN GW EP 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 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally,

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 and VPN GW EP 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 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 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the NDPP and VPN GW EP and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities 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 VPN GW EP, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each 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 VPN GW EP, 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.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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 VPN GW EP, and correctly verified that the product meets the claims in the ST.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

10 Validator Comments

The validation team notes that the evaluated configuration is dependent upon the ASR 1000 Series TOE being configured for FIPS operation.

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the devices are placed into the evaluated configuration. In particular, device administrators should ensure that all access controls lists (ACLs) contain a final rule to drop all unmatched traffic, and 256 bit keys may only be used for ESP tunnels when 256 bit keys are required for IKE negotiation

Administrative users must ensure that remote administrative SSH client is configured to use the approved cryptographic algorithms and MACs claimed in the evaluation, and are further recommended to restrict access to the TOE's SSH service to known clients.

The validation team notes that syslog on its own is an un-secured protocol, and in the evaluated configuration the TOE is expected to send its audit records to an external syslog server over an IPsec connection.

As was noted in the Clarification of Scope section of this report, the devices provide more functionality than was covered by the evaluation. Only the functionality claimed in the SFR's in the Security Target was evaluated. All other functionality provided by the devices needs to be assessed separately and no further conclusions should be drawn as to their effectiveness, nor can any claims be made relative to their security based upon this evaluation.

Conformance of RFC 768, 791, 793, and 2460 is vendor asserted.

11 Annexes

Not applicable

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

12 Security Target

The security target for this product's evaluation is *Cisco Aggregation Services Router (ASR) 1000 Series Security Target, Version 0.4, May 5, 2015*.

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

13 List of Acronyms

Acronym	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
BRI	Basic Rate Interface
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CSU	Channel Service Unit
DHCP	Dynamic Host Configuration Protocol
DSU	Data Service Unit
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

VALIDATION REPORT
Cisco Aggregation Services Router (ASR) 1000 Series

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	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 0.4, May 5, 2015.
6. Evaluation Technical Report for a Target of Evaluation “Cisco Aggregation Services Router (ASR) 1000 Series” Evaluation Technical Report v1.0 dated April 1, 2015.
7. Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance and Preparative Procedures, Version 0.4, May 5, 2015.
8. Assurance Activities Report for a Target of Evaluation Cisco Aggregation Services Routers (ASR) 1000 Series, Version 1.0, dated May 5, 2015