National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Cisco Systems, Inc.

170 W. Tasman Dr., San Jose, CA 95134

Cisco Aggregation Services Router (ASR) 900 Series

Report Number: CCEVS-VR-VID10599-2015

Dated: April 3, 2015

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Jerry Myers

Patrick Mallett

Common Criteria Testing Laboratory

Anthony Busciglio

Ashit Vora

1. Table of Contents

2. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Cisco's Aggregation Services Router (ASR) 900 Series. It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Acumen Security and completed in April 2015 The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

The Target of Evaluation (TOE) is the Cisco Aggregation Services Router (ASR) 900 series of products.

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 Protection Profile for Network Devices (NDPP) with Errata #2. 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. 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) 900 Series Security Target and analysis performed by the Validation Team.

3. 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) 900 Series
Protection Profile	U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1 with Errata #2
Security Target	Cisco Aggregation Services Router (ASR) 900 Series Security Target
Evaluation Technical Report	VID 10599 Common Criteria NDPP Assurance Activity Report, version 3.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Cisco Systems, Inc.
Developer	Cisco Systems, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Jerry Myers, Patrick Mallett

4. ARCHITECTURAL INFORMATION

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

The TOE consists of a number of components including:

- Chassis: The TOE chassis is designed for low power consumption, line rate performance for all Layer 2 and Layer 3 interfaces, the different hardware configuration options include 3-RU modular chassis and slots to support various cards and processors. There are also flexible clocking options, and redundant power and cooling. The chassis is the component of the TOE in which all other TOE components are housed.
- Route/Switch Processor (RSP) as noted above, this card the centralized card in the system performing the data plane, network timing, and control plane functions for the system. The four supported RSP cards, RSP1A-55, RSP1B-55, RSP2A-64 and RSP2A-128 are very similar in their performance, switching capabilities, interface (port) density, can be installed in both the ASR902 and ASR903. The differences are mainly in the services support scalability such as the amount of DRAM, the number of supported IP and multicast routes, MAC addresses, bridge domains and Ethernet flow points.
- Cisco IOS-XE software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Logical Scope of the TOE below.

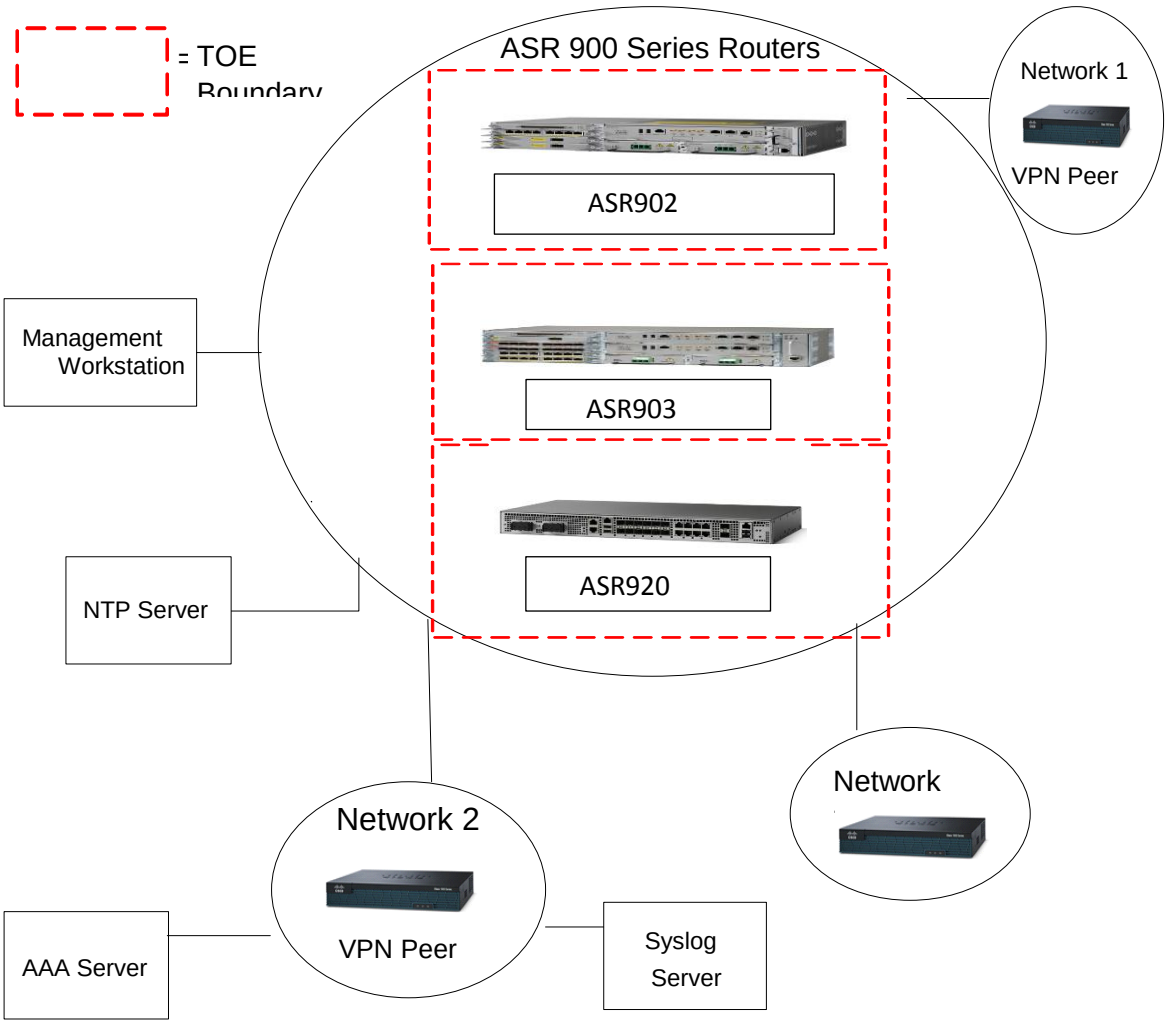
4.1. TOE DEPLOYMENT

The TOE consists of one or more physical devices as specified in section 3.2 below and includes the Cisco IOS-XE software. 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 TOE also provides timing services required in today's converged access networks by offering integrated support for the Building Integrated Timing Supply (BITS), 1 Pulse Per Second (1PPS) and Time Of Day (TOD) interfaces. The ASR 900 Series also supports Synchronous Ethernet (SyncE) and IEEE-1588 and can act as the source for network clocking for time-division multiplexing (TDM), Synchronous Digital Hierarchy (SDH), and Synchronous Optical Network (SONET), SyncE, and Global Positioning Satellite (GPS) interfaces. The ASR 900 Series router configuration will prioritize and process the data and signaling traffic for transport across the available networks. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

The TOE can optionally connect to an NTP server on its internal network for time services. Also, if the ASR 900 Series is to be remotely administered, then the management workstation station must be connected to an internal network, SSHv2 must be used to connect to the TOE. A syslog server is also used to store audit records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized

individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.



TOE Example Deployment

The previous figure includes the following:

- Examples of TOE Models (models listed in order of diagram)
  - Cisco ASR 902
    - 2-RU modular chassis
    - Dedicated slots in the chassis that support the following:

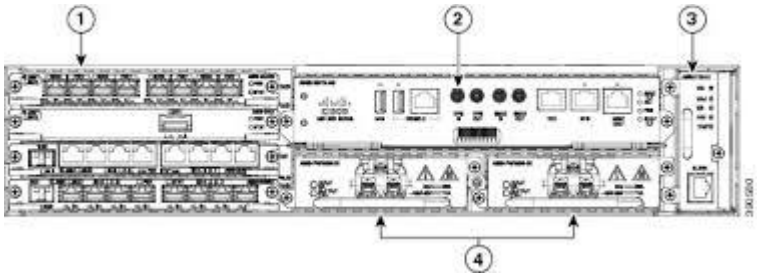
        - Up to four interface modules
        - One Route Switch Processor (RSP)
        - Up to two DC or two AC or a combination of AC and DC power supply units
        - One fan tray
    - Cisco ASR 903
        - 3-RU modular chassis
        - Dedicated slots in the chassis that support the following:
            - Up to six interface modules
            - Up to two Route Switch Processors (RSP)
            - Up to two DC power supply units
            - One fan tray
    - Cisco ASR 920
        - Indoor version includes ASR-920-12CZ-A and ASR-920-12CZ-D models that have fixed ENET interfaces (12 x 1GE + 2 x 10GE or 2 x 1GE or any combinations of 1 GE and 10 GE among the two ports available) and dual power supplies (AC/DC)
        - Compact version includes ASR-920-4SZ-A and ASR-920-4SZ-D models that have a compact form factor and configurable ports: 4 x 1 GE or 4 x 10 GE or any combinations of 1 GE and 10 GE among the four ports available. In addition, there are 2 x 1 GE copper ports available.
- 2 - Peer Routers (IT Environment)
- Management Workstation
- Syslog Server
- AAA Server
- NTP Server

NOTE: While the previous figure includes the available TOE devices and several non-TOE IT environment devices, the TOE is only the ASR 900 Series (902, 902 and 920) devices with the Cisco IOS-XE software. Only one TOE device is required in an evaluated configuration.

4.2. PHYSICAL SCOPE OF THE TOE

The TOE is a hardware and software solution that makes up the router models as described above in Section **Error! Reference source not found.**. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Aggregation Services Router (ASR) 900 Series Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site.

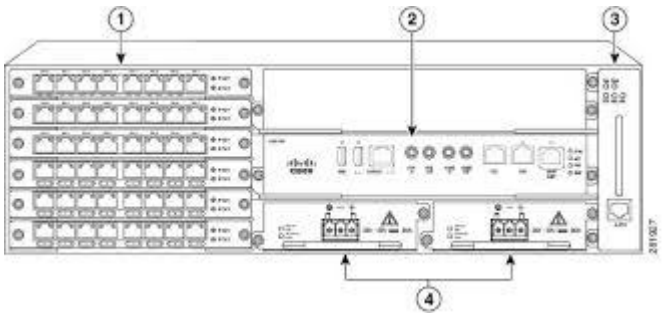
The TOE is comprised of the following physical specifications as described below:



ASR 902 chassis design

ASR 902 chassis References

Label	Component
1	Interface modules
2	One RSP unit slot; supports the RSP1A-55, RSP1B-55, RSP2A-64 and RSP2A-128
3	Fan tray
4	Redundant power units; two DC power units are shown

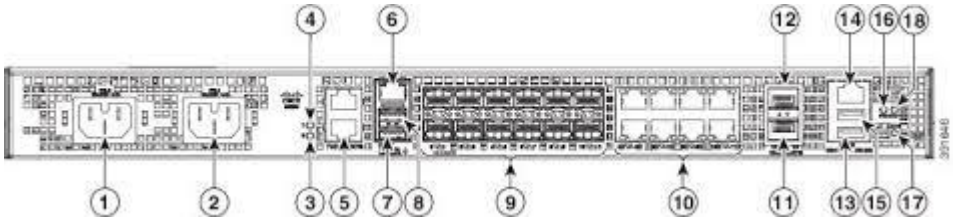


ASR 902 chassis design

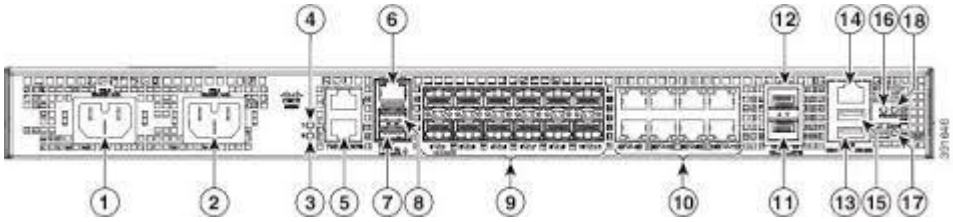
ASR 903 chassis References

Label	Component
1	Interface modules
2	Two RSP unit slots; supports the RSP1A-55, RSP1B-55, RSP2A-64 and RSP2A-128
3	Fan tray
4	Redundant power units; two DC power units are shown

ASR 920 chassis design



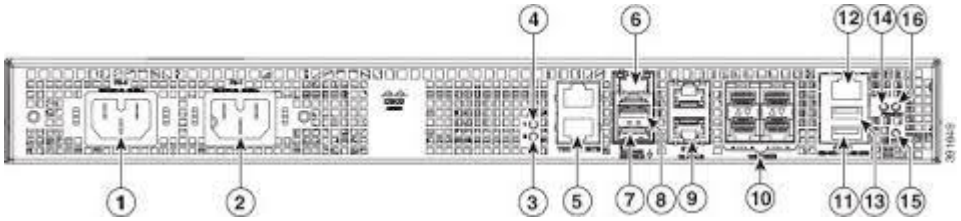
Front Panel of Cisco ASR-920-12CZ-A Router



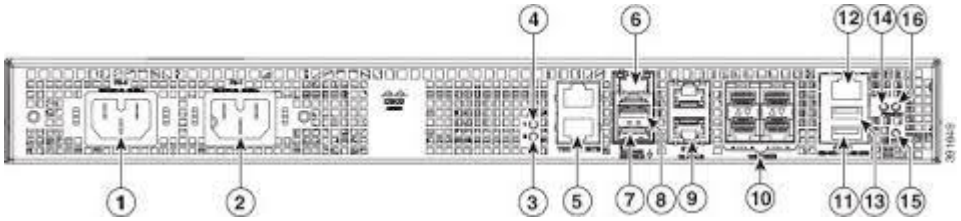
Front Panel of Cisco ASR-920-12CZ-D Router

ASR 920 (12CZ-A/12CD-D) chassis References

Label	Component	Label	Component
1	Power Supply 0 (AC or DC)	10	Eight Copper port
2	Power Supply 1 (AC or DC)	11	1G/10G Dual Rate port
3	Power Supply 0 LED (AC or DC)	12	1G/10G Dual Rate port
4	Power Supply 1 LED (AC or DC)	13	USB Console port
5	RJ-48 slots for BITS (upper slot) and ToD (lower slot)	14	Alarm port
6	Management port	15	USB Memory port
7	Console port (TIA/EIA-232F)	16	Board power LED
8	Auxiliary Console port	17	Zero Touch Provisioning button
9	4x1GE SFP + 8x1GE SFP combo ports	18	System Status LED



Front Panel of Cisco ASR-920-4SZ Router



Front Panel of Cisco ASR-920-4SZ -A Router

ASR 920 (4SZ/4SZ-A) chassis References

Label	Component	Label	Component
1	Power Supply 0 (AC or DC)	9	2 1GE Copper ports
2	Power Supply 1 (AC or DC)	10	Four 1G/10G Dual Rate ports
3	Power Supply 0 LED (AC or DC)	11	USB Console port
4	Power Supply 1 LED (AC or DC)	12	Alarm port
5	RJ-48 slots for BITS (upper slot) and ToD (lower slot)	13	USB Memory port
6	Management port	14	Board power LED
7	Console port (TIA/EIA-232F)	15	Zero Touch Provisioning button
8	Auxiliary Console port	16	System Status LED

The network, on which the TOE resides, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release IOS-XE 3.13.(1)S. 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.

4.3. LOGICAL SCOPE OF THE TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

1. Security Audit
2. Cryptography Support
3. User Data Protection
4. Identification & Authentication
5. Security Management
6. Protection of the TSF
7. Trusted Path/Channel
8. TOE Access

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDPP as necessary to satisfy testing/assurance measures prescribed therein.

4.3.1. Security Audit

The Cisco Aggregation Services Router (ASR) 900 Series provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event. Auditable events include: failure on invoking cryptographic functionality such as establishment, termination and failure of an IPsec SA; establishment, termination and failure of an SSH session; modifications to the group of users that are part of the authorized administrator roles; all use of the user identification mechanism; any use of the authentication mechanism; any change in the configuration of the TOE, changes to time, initiation of TOE update, indication of completion of TSF self-test, maximum sessions being exceeded, termination of a remote session and attempts to unlock a termination session; and initiation and termination of a trusted channel.

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE can be configured to block new permit actions.

The logs can be viewed on the TOE using the appropriate IOS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear audit data stored locally on the TOE.

4.3.2. Cryptographic Support

The TOE provides cryptography in support of other Cisco Aggregation Services Router (ASR) 900 Series security functionality.

This cryptography has been validated for conformance to the requirements of FIPS 140-2 (see **Error! Reference source not found.** for certificate references).

FIPS References

Algorithm	Cert. #
AES	2817
DRBG	481
SHS (SHA-1, 256, 384, 512)	2361
HMAC SHA-1, 256, 384, 512	1764
RSA	1471
ECDSA	493

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 **Error! Reference source not found.** below.

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.
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
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.

4.3.3. 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.

4.3.4. Identification & 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 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 TOEs 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 as well as mandatory password complexity rules. 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 or TACACS+ AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

4.3.5. 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:

- 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
- 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.

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.

4.3.6. 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. Additionally Cisco IOS is not a

general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS 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 synchronize the TOE's clock with an external time source. Finally, the TOE performs testing to verify correct operation of the switch 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 Authorized Administrator software.

4.3.7. TOE Access

The TOE can terminate 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.

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

4.3.8. Trusted Path/Channel

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.

4.4. EXCLUDED FUNCTIONALITY

The following functionality is excluded from the evaluation.

Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation on the	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet sends authentication data in the clear. This feature is enabled by default and must be disabled in the evaluated configuration. Including this feature would not meet the security policies as defined in the Security Target. The exclusion of this feature has no effect on the operation of the TOE. Refer to the Guidance documentation for configuration syntax and information

These services will be disabled by configuration. The exclusion of this functionality does not affect compliance to the compliance to the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 with Security Requirements for Network Devices Errata #2.

5. SECURITY POLICY

The security policies and functionality enforced by the TOE are described section 4.3 of this document.

6. ASSUMPTIONS AND CLARIFICATION OF SCOPE

6.1. ASSUMPTIONS

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

TOE Assumptions

Assumption	Assumption Definition
A.NO_GENERAL_PURPOSE	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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2. THREATS

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

Threats

Threat	Threat Definition
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.

6.3. OBJECTIVES

The following table, Security Objectives for the TOE, 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. An explanation of the relationship between the objectives and the threats/policies is provided in the rationale section of this document.

Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
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.

6.4. 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.
- 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 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 900 Series, with software version IOS-XE 3.13.(1)S. The TOE includes all the code that enforces the policies identified.

7. DOCUMENTATION

The following documents are available and required to configure the TOE in the evaluated configuration. Each of the following documents are available via www.cisco.com with the exception of the Security Target which is available via the NIAP website. No other documentation should be considered trusted for deploying the TOE in the evaluated configuration.

1. Cisco Aggregation Services Router (ASR) 900 Series Security Target [ST], version 1.0;
2. Cisco Aggregation Services Router (ASR) 900 Series Common Criteria Operational User Guidance and Preparative Procedures [AGD], version 1.0;
3. Release Notes for the ASR 900 Series; New Features for Cisco IOS XE Release 3.13 [NEW FEAT]
4. Cisco ASR 920 Series Aggregation Services Router Release Notes [RELEASE NOTES]
5. Cisco ASR 902 Aggregation Services Router Hardware Installation Guide [INIT CONF]
6. Cisco ASR 903 Router Hardware Installation Guide [903HW INSTALL]
7. Cisco ASR 920 Series Aggregation Services Router Hardware Installation Guide [920HW INSTALL]
8. Cisco IOS XE Configuration Fundamentals Configuration Guide, Release 2 [CONF FUND]
9. Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 900 Series) [MGT IMAGES]
10. Network Management Configuration Guide, Cisco IOS Release 15.0S [NETW CONF]
11. Cisco IOS Configuration Fundamentals Command Reference [IOSCONF FUND]
12. Basic System Management Configuration Guide, Cisco IOS XE Release 3S [BSM]
13. Configuration Fundamentals Configuration Guide Cisco IOS XE Release 3S [XE3SCONF FUN]
14. Cisco ASR 900 Router Series Configuration Guide [ASR900 CONF]
15. Cisco ASR 903 Router Chassis Software Configuration Guide, IOS XE Release 3.11S [CHASS CONF]
16. Configuration Fundamentals Configuration Guide, Cisco IOS Release 15.1S [15SCONF FUN]
17. Cisco IOS Security Command Reference [SEC COM]
18. Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS XE Release 3S [IKE CONF]
19. Basic System Management Configuration Guide, Cisco IOS XE Release 3S [XE3BSM]
20. LAN Routing Configuration Guide, Cisco IOS XE Release 3S [LAN CONF]
21. Secure Shell Configuration Guide, Cisco IOS XE Release 3S [SSH CONF]
22. User Security Configuration Guide, Cisco IOS XE Release 3S [USRSEC CONF]
23. Licensing the Cisco ASR 900 Series Routers [LIC CONF]

8. EVALUATED CONFIGURATION

The TOE consists of the following ASR 901 hardware models: ASR 902 and 903 including RSP (RSP1A-55, RSP1B-55, RSP2A-64 and RSP2A-128) and 920 (ASR-920-12CZ-A, ASR-920-12CZ-D, ASR-920-4SZ-A and ASR-920-4SZ-D) with IOS-XE 3.13(1)S software installed.

The TOE must be deployed as described in section 4.1 of this document and be configured as described in the Cisco Aggregation Services Router (ASR) 900 Series Common Criteria Operational User Guidance and Preparative Procedures [AGD].

9. IT PRODUCT TESTING

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for the Cisco ASR 900, which is not publically available. The Assurance Activities Report (available from the NIAP website) provides an overview of testing and the prescribed assurance activities.

9.1. DEVELOPER TESTING

The Assurance Activities of the NDPP version 1.1 with Errata #2 require that all evaluation results are based upon evaluator activities.

9.2. EVALUATION TEAM INDEPENDENT TESTING

The evaluation team verified the product according the guidance documentation identified in section 7 of this document.

Testing was performed on the following hardware,

- ASR 903 with a RSP1A-55 installed
- ASR 920 (Hardware model: ASR-920-4SZ-A)

The section 4 of the AAR (available via the NIAP website) provides an explanation of the equivalency analysis used to determine the hardware to be tested.

Three test beds were used for the product testing, as follows,

- The ASR 920 was tested at the Acumen Security facilities in Montgomery Village, Maryland using Testbed #1. The tester/evaluator had physical control of the TOE and test cases which were manually executed.
- A portion of the ASR 903 testing used Testbed #2. This testbed was located in the Cisco Systems facilities in Research Triangle, North Carolina. This testbed is functionally equivalent to testbeds #1 and #3.
- A portion of the ASR 903 testing used Testbed #3. These were tested on a testbed very similar to the testbed used in testing the ASR 920 (Testbed #1).

Sections 6 (for the ASR 903) and 7 (for the ASR 920) of the AAR provide a description of the test setup used for testing including,

- Visual depiction of the test bed,
- Description of the network addressing used,
- Test tools used,
- Test bed environment platforms including any installed software

Note: Because testbed #2 was provided by Cisco Systems, the specifics of the testbed are considered proprietary and may not be publically reproduced. The testbed however is functionally equivalent to testbeds #1 and #3.

Section 8 of the AAR provides a description of each test case executed by the tester with test step and results summaries.

10. 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 reader of this document can assume that 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 ASR 900 series to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

10.1. 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 900 series 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.

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.

10.2. 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. 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.

10.3. 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.

10.4. 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.

10.5. 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 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 that the conclusion reached by the evaluation team was justified.

10.6. 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.

10.7. 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.

11. VALIDATOR COMMENTS & RECOMMENDATIONS

Other than the items noted in section 6.4, “CLARIFICATION OF SCOPE”, the validators have no additional comments.

12. SECURITY TARGET

The security target for this product's evaluation is *Cisco Aggregation Services Router (ASR) 900 Series Security Target, Version 1.0, March 26, 2015*.

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 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) 900 Series Security Target, Version 1.0, March 26, 2015
6. [ETR] Cisco Aggregation Services Router (ASR) 900 Series Common Criteria Security Target Evaluation Technical Report, version 3.0
7. [Guidance Docs] Cisco Aggregation Services Router (ASR) 900 Series Common Criteria Operational User Guidance and Preparative Procedures [AGD], version 1.0
8. [AAR] VID 10599 Common Criteria NDPP Assurance Activity Report, version 3.0

15. List of Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

Table 1: Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CE	Carrier Ethernet
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command Line Interface
CM	Configuration Management
DH	Diffie-Hellman
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
GE	Gigabit Ethernet port
HA	High Availability (device or component failover)
HMAC	Hashed Message Authentication Code
HTTPS	Hyper-Text Transport Protocol Secure
IS-IS	Intermediate System to Intermediate System. An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains.
IT	Information Technology
LAN	Local Area Network
MEF	Metro-Ethernet Forum. A MEF defines Ethernet Virtual Connection (EVC) as an association between two or more user network interfaces that identifies a point-to-point or multipoint-to-multipoint path within the service provider network.
NDPP	Network Device Protection Profile
NTP	Network Time Protocol
OS	Operating System
OSPF	Open Shortest Path First. An interior gateway protocol (routes within a single autonomous system). A link-state routing protocol which calculates the shortest path to each node.
PP	Protection Profile
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network
VLAN	Virtual Local Area Network