National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Cisco Aggregation Services Router (ASR) 1000 Series, Version 1.0

Report Number: CCEVS-VR-10816-2017

Dated: 11/17/17

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

Jerome Myers

Kenneth Stutterheim

Meredith Hennan

The Aerospace Corporation

Common Criteria Testing Laboratory

Kevin Micciche

Zalman Kuperman

Kevin Zhang

Acumen Security, LLC

Table of Contents

1 Executive Summary 5

2 Identification 6

3 Architectural Information 7

3.1 TOE Evaluated Platforms 7
3.2 TOE Architecture 8
3.3 Physical Boundaries 9

4 Security Policy 10

4.1 Security Audit 10
4.2 Cryptographic Support 10
4.3 Identification and Authentication 11
4.4 Security Management 12
4.5 Protection of the TSF 13
4.6 TOE Access 13
4.7 Trusted Path/Channel 13

5 Assumptions, Threats & Clarification of Scope 14

5.1 Assumptions 14
5.2 Threats 15
5.3 Clarification of Scope 17

6 Documentation 18

7 TOE Evaluated Configuration 19

7.1 Evaluated Configuration 19
7.2 Excluded Functionality 19

8 IT Product Testing 20

8.1 Developer Testing 20
8.2 Evaluation Team Independent Testing 20

8.2.1 Test Bed 1 20

8.2.2 Test Bed 2 21

9 Results of the Evaluation 23

9.1 Evaluation of Security Target (ASE) 23
9.2 Evaluation of Development Documentation (ADV) 23
9.3 Evaluation of Guidance Documents (AGD) 23
9.4 Evaluation of Life Cycle Support Activities (ALC) 24
9.5 Evaluation of Test Documentation and the Test Activity (ATE) 24
9.6 Vulnerability Assessment Activity (VAN) 24
9.7 Summary of Evaluation Results 25

10 Validator Comments & Recommendations 26

11 Annexes 27

12 Security Target 28
13 Glossary 29
14 Bibliography 30

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Cisco Aggregation Services Router (ASR) 1000 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in November 2017. 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 defined in the U.S. Government Protection Profile for Security Requirements for the collaborative Protection Profile for Network Devices version 1.0 (NDcPPv1.0).

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 NDcPP 1.0. 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 (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). 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). Based on these findings, 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.

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 Common Evaluation Methodology (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
Protection Profile	collaborative Protection Profile for Network Devices, version 1.0, February 27, 2015 (NDcPPv1.0)
Security Target	Cisco Aggregation Services Router (ASR) 1000 Series Security Target, version 0.7, October 17, 2017
Evaluation Technical Report	Cisco Aggregation Services Router (ASR) 1000 Series ETR, version 1.2, November 17, 2017
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	Jerome Myers, Kenneth Stutterheim, Meredith Hennan *The Aerospace Corporation*

3 Architectural Information

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

The Cisco ASR1K Series delivers embedded hardware acceleration for multiple Cisco IOS-XE Software services. In addition, the Cisco ASR1K Series Router features redundant Route and Embedded Services Processors, as well as software-based redundancy. In support of the routing capabilities, the Cisco ASR1K provides IPsec connection capabilities to facilitate secure communications with external entities, as required.

The hardware models included in the evaluation are: 1004. The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 4-RU form factor. The chassis is the component of the TOE in which all other TOE components are housed.
- Embedded Services Processor (ESPr): The Cisco ASR1K Series ESPrs (ESP10, ESP 20, ESP40) are responsible for the data-plane processing tasks, and all network traffic flows through them.
- Route Processor (RP): The Cisco ASR1K Series RPs (RP1 and RP2) provide the advanced routing capabilities of the TOE. They also monitor and manage the other components in the Cisco ASR1K Series Aggregation Services.
- Shared Port Adaptors (SPAs): Used for connecting to networks. These SPAs interface with the TOE to provide the network interfaces that will be used to communicate on the network.

3.1 TOE Evaluated Platforms

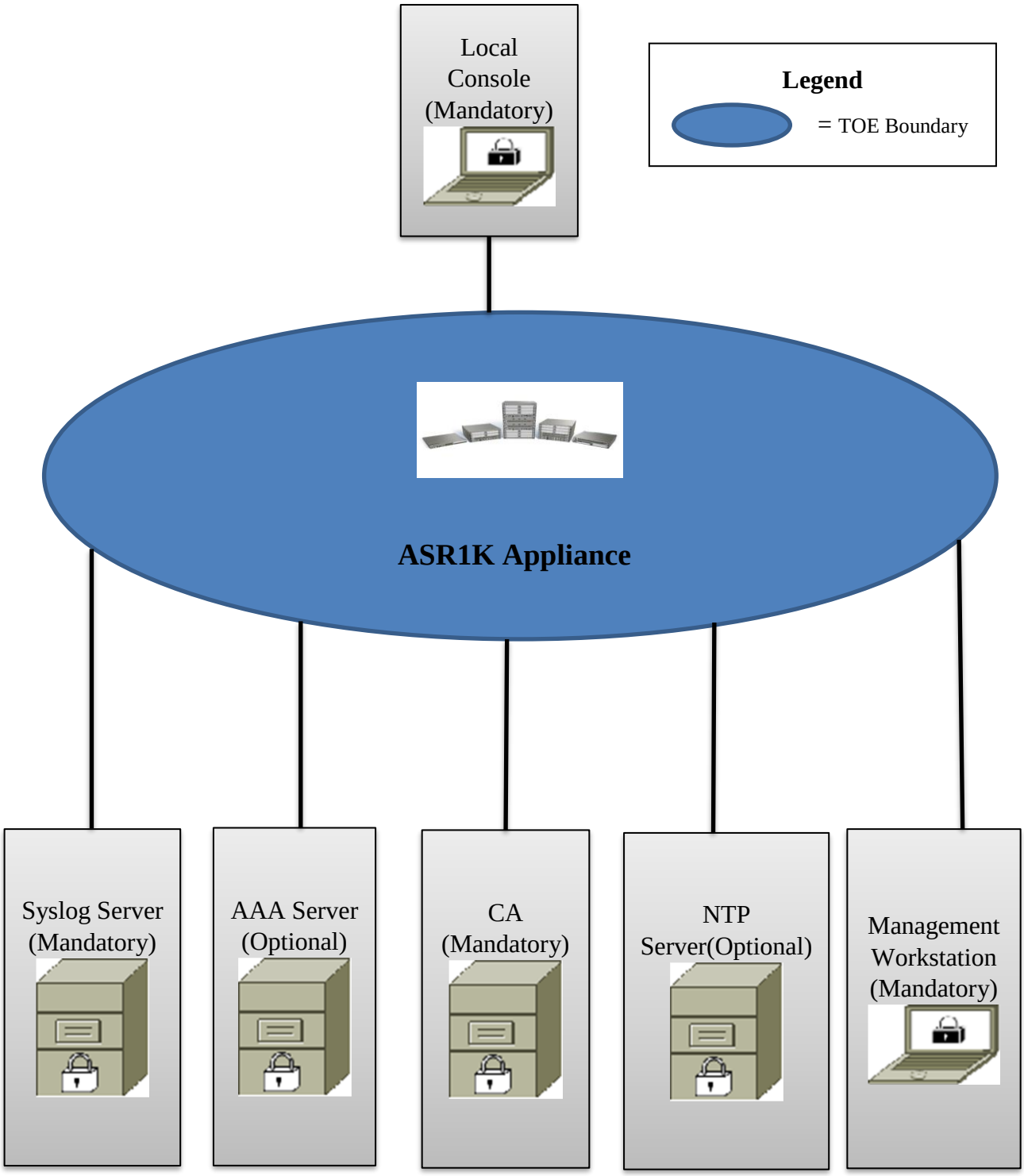
The TOE is a hardware and software solution that makes up the router models as follows: Chassis:

- ASR 1004; Embedded Services Processors (ESP): ESP20 and ESP40; Route Processor (RP): RP1, RP2

3.2 TOE Architecture

The following figure provides a visual depiction of an example TOE deployment.

Figure 1 TOE Example Deployment



The following are considered to be in the IT Environment:

- Management Workstation
- Authentication Server
- NTP Server
- Syslog Server
- Local Console
- CA

NOTE: While the previous figure includes several TOE devices and several non-TOE IT environment devices, the TOE is only the ASR1K device. Only one TOE device is required for deployment of the TOE in an evaluated configuration.

3.3 Physical Boundaries

The TOE is comprised of the following physical specifications as described in Table 2 below:

Table 2: ASR1K Hardware Models and Specifications

Hardware Model	ASR 1004
Dimensions (HxWxD) in inches	7 x 17.2 x 18.15
Shared Port Adapters	8
Ethernet Port Adapters	n/a
Embedded services processor slots	1
ESP Bandwidth	10 to 40 Gbps
Route processor slots	1
Built-in Gigabit Ethernet ports	0
Default memory	4-GB DRAM RP1 8-GB DRAM RP2
External USB flash memory	1-GB USB flash-memory support

4 Security Policy

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. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Packet Filtering
6. Protection of the TSF
7. TOE Access
8. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

4.1 Security Audit

The ASR1K provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE 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.

4.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates.

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 the table below.

Table 3: 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
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

4.3 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.

4.4 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.

4.5 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 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.

4.6 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.

4.7 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, as well as to protect communications with a CA or remote administrative console.

5 Assumptions, Threats & Clarification of Scope

5.1 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.

Table 4: TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

5.2 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.

Table 5: Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

Threat	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself. An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.

Threat	Threat Definition
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5.3 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 NDcPP 1.0.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- 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 and applicable Technical Decisions. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Cisco Aggregation Services Router (ASR) 1000 Series Security Target, version 0.7, October 17, 2017
- Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures, version 0.5, September 27, 2017

Any additional customer documentation delivered with the product or that is available through download was not included in the scope of the evaluation, and therefore should not be relied upon when configuring or using the products as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a hardware and software solution that makes up the router models as follows:
Chassis:

- ASR 1004; Embedded Services Processors (ESP): ESP20 and ESP40; Route Processor (RP): RP1, 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 16.3, and configured in accordance with the AGD [8]. 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.

7.2 Excluded Functionality

In addition to any functionality not covered by Security Functional Requirements (SFRs) in the NDcPPv1.0, the following functionality is excluded from the evaluation:

Table 6: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

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 proprietary Test Plan for a Cisco ASR 1004 NDcPP 1.0, and summarized in the Common Criteria NDcPP Assurance Activity Report for Cisco Aggregation Services Router (ASR) 1000 Series, version 1.3, November 11, 2017 (AAR), which is publicly available.

8.1 Developer Testing

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

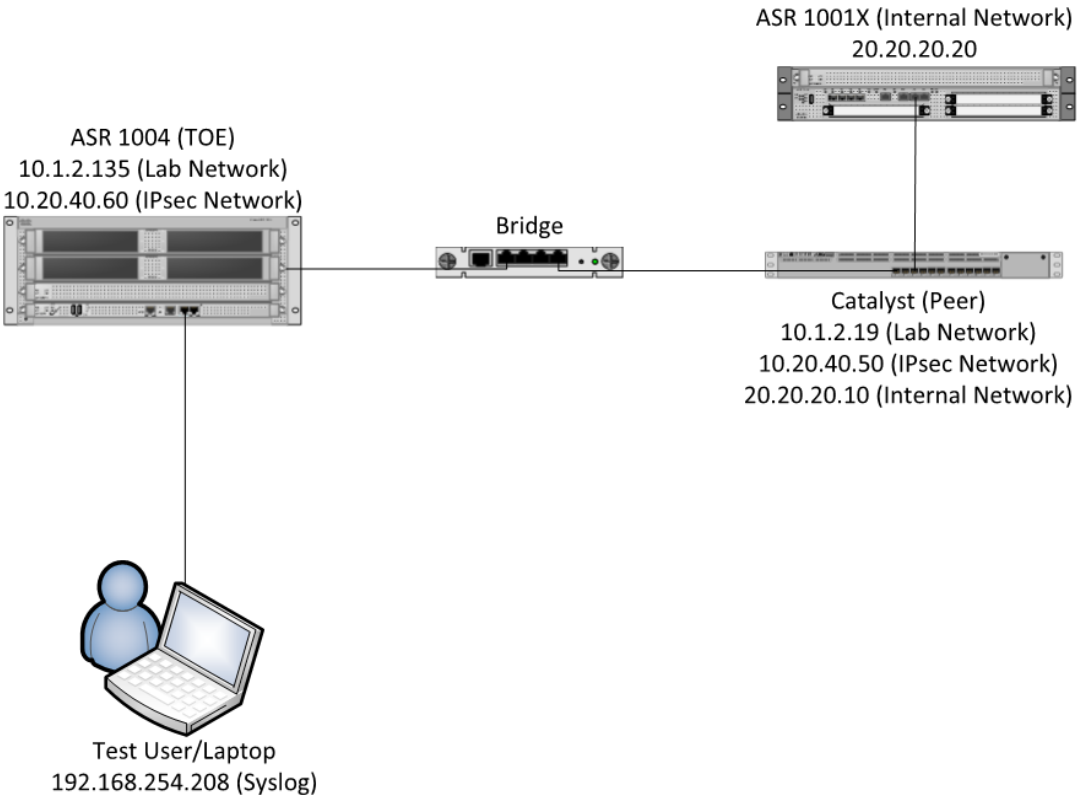
8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the NDcPP 1.0. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

The following is the test infrastructure used by the evaluators:

8.2.1 Test Bed 1

Figure 2: Test Bed 1



8.2.1.1 Configuration Information

The following provides configuration information about each test device and test tool on the test network.

8.2.1.1.1 Cisco ASR 1004

- Software Version: IOS-XE 16.3
- IP Address: 10.20.40.60, 10.1.2.135

8.2.1.1.2 Cisco Catalyst 3650

- Software Version: Cisco IOS-XE 16.3
- IP Address: 10.20.40.50, 10.1.2.19, 20.20.20.10

8.2.1.1.3 Cisco ASR 1001X

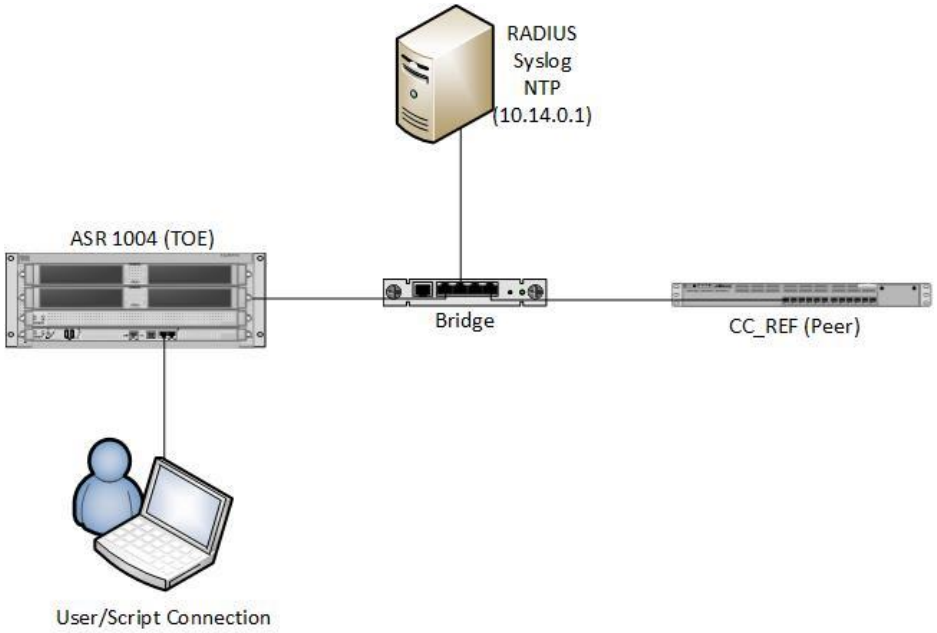
- Software Version: Cisco IOS-XE 16.3
- IP Address: 20.20.20.20

8.2.1.1.4 Test Laptop

- Software Version: Windows 10
- IP Address: 192.168.254.208
- Ubuntu 64-bit (running in VMware Workstation Player 12)
- Kiwi Syslog Server 9.6
- Wireshark 2.2.6
- Putty 0.68

8.2.2 Test Bed 2

Figure 3: Test Bed 2



8.2.2.1 Configuration Information

The following provides configuration information about each test device and test tool on the test network.

8.2.2.1.1 Cisco ASR 1004

- Software Version: IOS-XE 16.3
- IP Address: Varied based on test script run:
    - 10.32.0.X (IPsec)
    - 10.11.0.110 (SSH)
    - 10.10.10.1 (Telnet)
    - 10.41.0.110
    - 10.44.0.1
    - 10.21.0.110
    - 10.22.0.210
    - 10.12.0.210

8.2.2.1.2 CC_REF

- Software Version: Cisco IOS-XE 16.3
- IP Address: Varied based on test script run:
    - 10.13.0.1
    - 10.33.0.X
    - 10.11.0.101
    - 10.41.0.401
    - 10.43.0.1
    - 50.0.0.1
    - 10.22.0.2
    - 10.42.0.X

8.2.2.1.3 Test User Laptop

- IP Address: 10.11.0.103

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 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 Aggregation Services Router (ASR) 1000 Series to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDcPP1.0.

9.1 Evaluation of Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Aggregation Services Router (ASR) 1000 Series 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 NDcPP 1.0.

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 Development Documentation (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 NDcPP 1.0 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 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, 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 NDcPP 1.0 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 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 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 NDcPP 1.0 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 NDcPP 1.0, 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 vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities did not uncover any residual vulnerability.

The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below.

- http://nvd.nist.gov/
- http://www.us-cert.gov
- http://www.securityfocus.com/

The evaluator performed the public domain vulnerability searches using the following key words.

- Aggregation Services Router
- IOS-XE 16.3
- ASR1k

- ASR 1004

The evaluator selected the search key words based upon the following criteria.

- The vendor name was searched,
- The software running on the TOE devices were searched. Further, the version the TOE software in evaluation was searched,
- The name of the hardware devices within the TOE,
- The secure protocols supported by the TOE,
- The type of TOE device.

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 NDcPP 1.0, and that the conclusion reached by the evaluation team was justified. This analysis was performed and completed in October 2017 and reviewed prior to issuing of the certificate.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the NDcPP 1.0, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

All validator comments have been addressed in the Assumptions and Clarifications of Scope sections.

11 Annexes

Not applicable.

12 Security Target

Cisco Aggregation Services Router (ASR) 1000 Series Security Target, version 0.7, October 17, 2017.

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) 1000 Series Security Target, version 0.7, October 17, 2017. (ST)
6. Common Criteria NDcPP Assurance Activity Report for Cisco Aggregation Services Router (ASR) 1000 Series, version 1.3, November 11, 2017 (AAR)
7. Cisco Aggregation Services Router (ASR) 1000 Series ETR, version 1.2, November 17, 2017 (ETR)
8. Cisco Aggregation Services Router (ASR) 1000 Series Common Criteria Operational User Guidance And Preparative Procedures, version 0.5, September 27, 2017 (AGD)