Certificate Report

Version 1.0

15 May 2023

CSA_CC_20003

For

Huawei NetEngine AR6121 and AR6121E Routers, V300R019C13

From

Huawei Technologies Co. Ltd.

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	15 May 2023	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Huawei NetEngine AR6121 and AR6121E Routers, V300R019C13, Network Device, and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Hardware	AR6121
	AR6121E
Firmware	V300R019C13

Table 1 - TOE components identifier

The AR6121 and AR6121E routers have identical software architecture and hardware components with the only difference being the device memory (SDRAM) capacity; AR6121E is equipped with 4GB SDRAM whereas AR6121 is equipped with 2GB SDRAM.

The TOE is a network routing engine and gateway device, which provides routing (i.e., RIP, OSPF, ISIS, and BGP routing protocols), switching, wireless communication, and security functions.

The TOE can be used for Layer 2 forwarding and Layer 3 forwarding purposes. When working as Layer 2 forwarding devices, the forwarding engine of TOE will forward the traffic according to MAC address. When working as Layer 3 forwarding devices, The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine.

The list of guidance documents to use with the product in its certified configuration is as follows.

Name	Version	Method of Delivery
NetEngine AR V300R019 Product Documentation Format: webpage or .hdx (Huawei product documentation format, can be opened using HedEx Lite) Users can login the HUAWEI support website to view the documentation or download the document and open using HedEx Lite	V300R019	Website: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100087043&lang=en

Table 2 - List of guidance documents

The TOE uses a quad-core Central Processing Unit (CPU) whereby Core 0 is dedicated for control and management process, while the remaining CPU cores (1, 2 & 3) are dynamically allocated to forwarding and service processes.

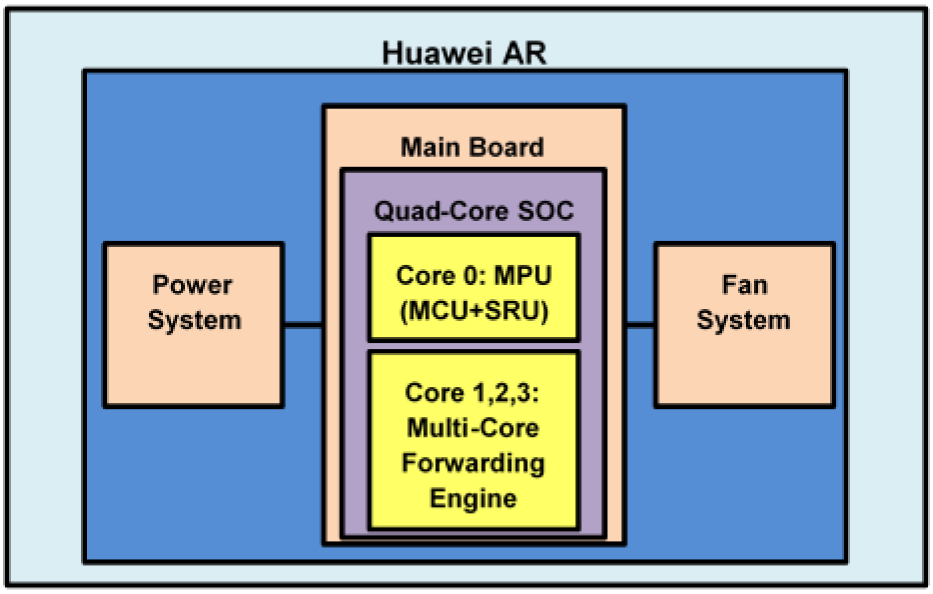

Figure 1: TOE Physical Architecture

The scope of evaluation is the Huawei NetEngine AR6121 and AR6121E routers, which consists of device hardware and firmware.

The evaluation of the TOE has been carried out by UL Verification Services Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL 2 augmented with ALC_FLR.2 (Flaw Reporting Procedures) and completed on 11 May 2023.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
Authentication Enforces administrative users authentication by username and password for virtual terminal sessions via SSH, and S-FTP (Secured FTP) sessions, as well as authentication via the console.
Access Control Enforces access control by four hierarchical administration levels. The TOE can either decide the authorization level of a user based on its local database.
L2 Traffic Forwarding Handles Layer 2 forwarding policy and controls the flow of network packets by enforcing a decision with regards to the network interface that a packet gets forwarded to, based on a MAC table maintained by administrators (static MAC) or updated dynamically by MAC learning function when an unknown MAC address packet has been received.
L3 Traffic Forwarding Handles Layer 3 forwarding policy and controls the flow of network packets by enforcing a decision with regards to the network interface that a packet gets forwarded to, based on a routing table maintained by administrators (static routing) or updated dynamically by the TOE when exchanging routing information with peer routers. The TOE support IPsec protocol. By authenticating and encrypting each IP packet in the data flow, the IP datagram is provided with interoperable, and password-based security.
Audit Generates audit records for security-relevant management actions and stores the audit records in flash in the TOE.
Communication Security Provides communication security by implementing SSH2 (SSH2.0) to protect TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH2 provides: • authentication by password, by RSA or by password with RSA; • AES encryption algorithms • Secure cryptographic key exchange by DH-group14-sha256 • HMAC-SHA256 is used as verification algorithm for SSH. Provides S-Telnet and S-FTP to implement secure Telnet and FTP. Provides IPsec protocol to protect IP packets forwarding, IPsec provides: • Key-exchange: Group 14(2048 bits) and Group 21(521-bits ECP) • AES-CBC-256 encryption algorithms.

- Integrity: hmac-sha2-512
- Digital Signature: PSS and PKCS1

Access Control List

Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces.

The administrator can create, delete, and modify rules in ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE or other network devices through interfaces by matching information contained in the headers of connection-oriented or connectionless packets against that specified in the ACL rules.

Source MAC address, Destination MAC address, Ethernet protocol type, Source IP address, destination IP address, IP protocol number, source port number (if TCP/UDP protocol is in use), destination port number (if TCP/UDP protocol is in use), TCP flag (if TCP protocol is in use), type and code (if ICMP protocol is in use), fragment flag etc., can be used for ACL rule configuration.

If no rule is created in an ACL, the ACL cannot match any traffic. If no ACL or ACL rule is configured, the TOE performs the following operations based on features:

1. For filtering features (such as Telnet), if no ACL is configured, login is allowed by default.
2. By default, the prioritize and rate-limit are not adjusted, and the original forwarding mode is used.

Security Functionality Management

Security functionality management includes authentication, access level, managing security related data consisting of configuration profile and runtime parameters. More functionalities incudes,

More functionalities include:

- Setup to enable SSH2.0.
- Setup to enable BGP, OSPF, ARP.
- Setup to enable audit, as well as suppression of repeated log records.
- Setup to change default rate limit plan.

In addition to management of TSF, the TOE also supports Network event report using Simple Network Management Protocol (SNMP). The TOE uses SNMP traps to notify a fault occurs or the system does not operate properly.

Cryptographic Functions Supports Cryptographic functions required by security features as dependencies, where: 1. AES256 is used as default encryption algorithm for SSH. 2. RSA is used in user authentication when user tries to authenticate and gain access to the TOE. 3. SHA256 is used as option HMAC algorithm for SSH. 4. HMAC-SHA256 is used as verification algorithm for packets of BGP and OSPF protocols from peer network devices.
Packet Filtering Supports packet filtering which filters packets through ACLs, based on upper-layer protocol number, source and destination IP addresses, source and destination port numbers, and packet direction. TOE internetworking devices are deployed at the edges of untrusted networks (such as the Internet), to provide controlled communications between two networks that are physically separated. When a packet flow reaches the TOE, the TOE applies an information flow security policy in the form of access control lists and stateful inspection to the traffic before forwarding it into the remote network. Packet flows arriving at a network interface of the TOE are checked to ensure that they conform with the configured packet filter policy, this may include checking attributes such as the presumed source or destination IP address, the protocol used, the network interface the packet flow was received on, and source or destination UDP/TCP port numbers. Packet flows not matching the configured packet filter policy are dropped.

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till 1**4 May 2028**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: Huawei NetEngine AR6121 and AR6121E Routers Version V300R019C13.

The following table identifies the TOE deliverables.

Identifier	Version
Hardware	AR6121
	AR6121E
Firmware	V300R019C13

Table 4 - TOE Deliverables

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name	Version	Method of Delivery
NetEngine AR V300R019 Product Documentation Format: webpage or .hdx (Huawei product documentation format, can be opened using HedEx Lite) Users can login the HUAWEI support website to view the documentation or download the document and open using HedEx Lite	V300R019	Website: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100087043&lang=en

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	Huawei NetEngine AR6121 and AR6121E Routers Version V300R019C13
sSecurity Target	Huawei NetEngine AR6121 and AR6121E, V300R019C13 Routers Security Target Version 1.4, 27 Mar 2023
Developer	Huawei Technologies Co., Ltd.
Sponsor	Huawei Technologies Co., Ltd.
Evaluation Facility	UL Verification Services Pte Ltd
Completion Date of Evaluation	11 May 2023
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_20003
Certificate Validity	5 years from date of issuance

Table 6: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Resource Utilisation
- TOE Access
- Trusted Path/Channels

Specific details concerning the above mentioned security policy can be found in Chapter 1.4.3 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.NetworkElements	The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other routers for the exchange of routing information, PCs used for TOE administration and NTP server for providing reliable time source.
OE.Physical	The TOE (i.e., the complete system including attached peripherals, such as a console shall be protected against unauthorized physical access
OE.NetworkSegregation	The operational environment shall provide segregation by deploying the ETH interface in TOE into a local sub-network, compared to the network interfaces in TOE serving the application (or public) network.
OE.Person	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the TOE.

Table 7: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

The TOE supports the use of external Radius and TACACS+ server for user authorisation information, however this configuration is outside the scope of this evaluation. Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

5.3 Evaluated Configuration

The TOE is a network device which provide routing, switching, wireless communication, and security functions. It offers a platform for scalable multi-service integration at enterprise and commercial branch offices and small-to-medium sized businesses. The TOE's supported routing protocols are RIP, OSPF, ISIS, and BGP.

The AR6121 and AR6121E routers have identical software architecture and hardware components with the only difference being the device memory (SDRAM) capacity: AR6121E is equipped with 4GB SDRAM whereas AR6121 is equipped with 2GB SDRAM.

The TOE can be used for Layer 2 forwarding and Layer 3 forwarding purposes. When working as Layer 2 forwarding devices, the forwarding engine of TOE will forward the traffic according to MAC address. When working as Layer 3 forwarding devices, The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine.

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE requires additional components (i.e., hardware/software/firmware) for operation. These non-TOE components include:

- Switches and Routers
- Local Network Management System (NMS) Workstation
  (For Local Management)
- Remote Network Management System (NMS) Workstation
  (For Remote Management)
- Physical Network
- NTP Server

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

The Versatile Routing Platform (VRP) is responsible for managing and running the router's networking functionality and uses VP (Virtual Path) to link up the data forwarding plane. The VRP provides security features such as access control; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The VRP is deployed on the Main Processing Unit[2] (MPU) within Core 0 of the Quad-Core System-on-Chip (SoC), while Core 1 to 3 forms the forwarding engine that determines how packets are handle to and from the router's network interface.

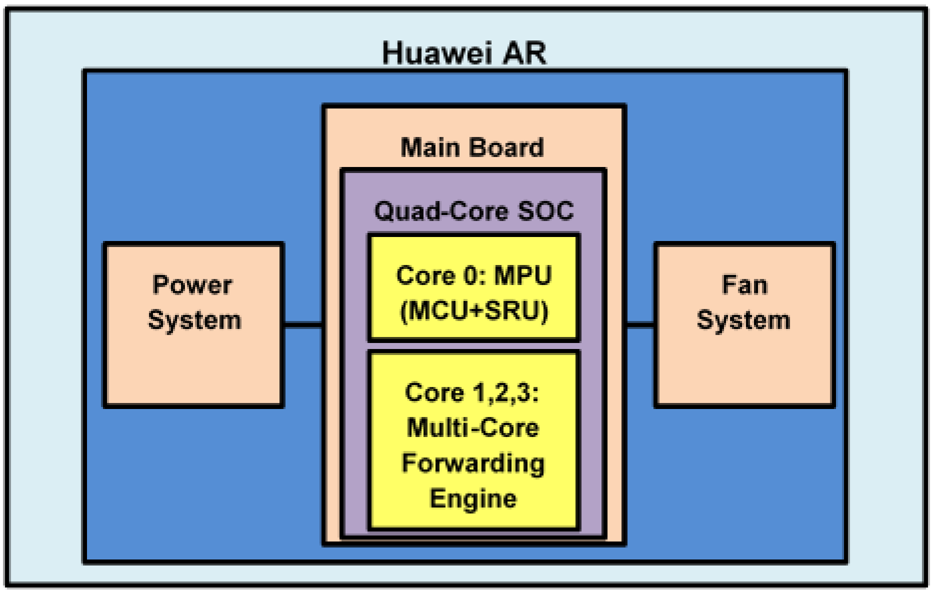

Figure 2- TOE Architecture

[2] The MPU consists of the MCU (Main Control Unit) and SRU (Switch Routing Unit)

The TOE's software architecture consists of the following logical planes to support centralised forwarding and control and distributed forwarding mechanism.

- Data Plane (DFP, Routing table, MAC Address table)
- Control and Management plane (SCP, SMP, GCP)

The Control and Management plane processes protocols and signals, configures, and maintains the system status, and reports and controls the system status. The Data Plane is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, forwards IPv4/IPv6 packets, performs Quality of Service (QoS) and scheduling, completes inner high-speed switching, and collects statistics.

The monitoring plane (Non-TSF) monitors the system environment by detecting the voltage, controlling power-on and power-off of the system, and monitoring the temperature and controlling the fan, and send an alarm to the customer while system overload occurs. For example, the fan speed increases when the temperature increases, and the fan speed decreases when the temperature decreases. When the temperature is too high or too low or the fan is faulty, the device sends an alarm.

The System Service Plane (SSP) (Non-TSF) provides the abstract layer of the operating system so that the VRP can be independent of the specific operating system.

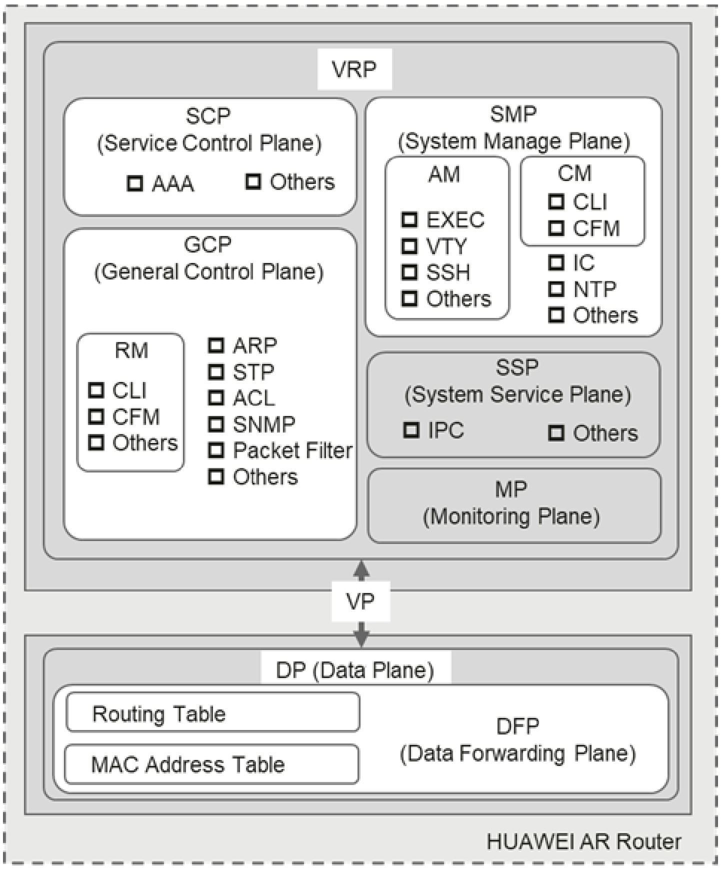

Figure 3 - TOE Software Architecture

7 Documentation

The evaluated documentation as listed in

Name	Version	Method of Delivery
NetEngine AR V300R019 Product Documentation Format: webpage or .hdx (Huawei product documentation format, can be opened using HedEx Lite) Users can login the HUAWEI support website to view the documentation or download the document and open using HedEx Lite	V300R019	Website: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100087043&lang=en

Name	Version	Method of Delivery
NetEngine AR V300R019 Product Documentation Format: webpage or .hdx (Huawei product documentation format, can be opened using HedEx Lite) Users can login the HUAWEI support website to view the documentation or download the document and open using HedEx Lite	V300R019	Website: https://support.huawei.com/hedex/hdx.do?docid=EDOC1100087043&lang=en

Table 5 - Guidance Document (part of TOE deliverables) is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The evaluator sampled and repeated the developer's testing related to TSFIs and TSFs to ensure that the TSF implemented are correct. The evaluator installed the TOE by following evaluation confirmation requirement and then reproduced the developers testing to verify the results.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9] [10] [11].

In most of the test cases, a Huawei AR6121/AR6121E router is setup on a local area network where communication is allowed between the evaluator's PC and the Huawei AR6121/AR6121E router. Figure 3 illustrate the TOE testing environment.

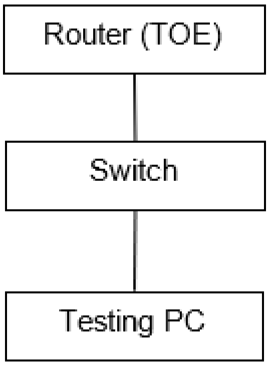

Figure 3 – TOE Test Configuration

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The evaluator conducted a set of independent tests to supplement or augments the developer's existing test plan.

The evaluator's strategy for devising independent tests was based on the following:

1. To review developer test evidence.
2. To make sure that the tests cover all the SFR-enforcing TSFIs.
3. To make sure that the TSF operates as per functional specification described.
4. To maintain a balance of evaluation activities by considering the evaluator effort expended on the test activity and any other evaluation activity.
5. Referred to similar product evaluation guide, such as NDcPP.
6.

8.2.2 Test Configuration

A detailed test description was provided in the ATE document. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

8.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The evaluator performed a public vulnerability search, including a literature review of conference proceedings, University research, relevant journals, published papers, any blogs and writeups. The evaluator also considered Internet surveys and online vulnerability databases

The evaluator reviewed the identified potential vulnerabilities and performed an independent vulnerability analysis of the TOE documentation

The evaluator devised attack scenario based on these potential vulnerabilities and performed theoretical analysis on the related attack potential including attack scenarios with basic or slightly above basic attack potential.

Penetration Test	Description
Test Case #1	Potential vulnerabilities on SNMPv3 Service
Test Case #2	Escalation of command line rights

Table 6 - Penetration Test Case

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

9 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 augmented by ALC_FLR.2 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

The TOE supports the use of external Radius and TACACS+ server for user authorisation information, however this configuration is outside the scope of this evaluation.

Users are reminded to set up the TOE as per guidance documents (such as to enable firmware verification upon boot up) to correctly deploy and use the TOE in the evaluated configuration.

No additional recommendation was provided by the evaluators.

11 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

12 Bibliography

[1] Huawei, "Huawei NetEngine AR6121 and AR6121E, V300R019C13 Routers Security Target, Version 1.6," 11 May 2023.

[2] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5," 2017.

[3] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5," 2017.

[4] Common Criteria Maintenance Board (CCMB), "Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5," 2017.

[5] Common Criteria Maintenance Board (CCMB), "Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5," 2017.

[6] Cyber Security Agency of Singapore (CSA), "SCCS Publication 1 - Overview of SCCS, Version 5.0," 2018.

[7] Cyber Security Agency of Singapore (CSA), "SCCS Publication 2 - Requirements for CCTL, Version 5.0," 2018.

[8] Cyber Security Agency of Singapore (CSA), "SCCS Publication 3 - Evaluation and Certification, Version 5.0," 2018.

[9] Huawei, "Huawei NetEngine AR6121(E) V300R019C13 Routers Operational User Guidance, Version 1.9," 26 Apr 2022.

[10] Huawei, "Huawei NetEngine AR6121&AR6121E Routers V300R019C13 Preparative Procedures, Version 2.0," 11 Novemeber 2022.

[11] Huawei, "Huawei NetEngine AR6121(E) Routers V300R019C13 Configuration and Reference, Version 0.4," 23 March 2022.

---End of Report --