EUCC Certification Report

Huawei ATN Series Routers, version V800R022C00SPC600

Sponsor and developer:	***Huawei Technologies Co., Ltd*** **Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, People's Republic of China**
Evaluation facility:	***SGS Brightsight B.V*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**EUCC-3110-2025-11-2500051-01 Certification Report**
Report version:	**1**
Project number:	**EUCC-2500051-01**
Author(s):	**Andy Brown, TrustCB B.V.** **contact: eucc@trustcb.com**
Date:	**14 November 2025**
Number of pages:	**14**
Number of appendices:	**0**

CONTENTS

Foreword

The Common Criteria-based European Cybersecurity Certification Scheme (EUCC) is a certification scheme created under the Cybersecurity Act (CSA), Regulation (EU) 2019/881 of 17 April 2019.

The EUCC is described by Commission Implementing Regulation (EU) 2024/482 of 31 January 2024, laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC).

The Dutch implementation of the CSA is regulated in Dutch law in the 'Uitvoeringswet cyberbeveiligingsverordening' (UITVW). In this law the role of NCCA is assigned to the Dutch Authority for Digital Infrastructure (RDI), which is part of the Ministry of Economic Affairs.

TrustCB B.V. has been licensed by the RDI as a Certification Body (CB) for the task of ISO/IEC 17065 Certification Activities up to and including CSA assurance level high for ICT security products, as well as for protection profiles. Part of the procedure is the technical examination (evaluation) of the product, protection profile according to the NP002 EUCC processes published by the Dutch NCCA.

Evaluations of ICT products are performed by an IT Security Evaluation Facility (ITSEF) licensed by the Dutch NCCA as a CAB for ISO/IEC 17025 Evaluation Activities, with scope aligning to the requested Evaluation Assurance Level of the Object for the evaluation, referred to as the Target of Evaluation (TOE) in this report.

By awarding an EUCC certificate as a Common Criteria certificate, TrustCB B.V. asserts that the ICT product complies with the security requirements specified in the associated security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the ICT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the ICT product satisfies the security requirements stated in the security target.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei ATN Series Routers, version V800R022C00SPC600.

The developer of the Huawei ATN Series Routers, version V800R022C00SPC600 is Huawei Technologies Co., Ltd located in Shenzhen, People's Republic of China and they also act as the sponsor of the evaluation and certification.

A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is a series of network infrastructure routers including both hardware and software. It is defined as the software running on the hardware corresponding to the following routers: ATN 910C-M, ATN 910C-K and ATN 910D-B. These routers consist of both hardware and software.

The TOE has been evaluated by SGS Brightsight B.V located in Delft, The Netherlands. The evaluation was completed on 10 October 2025 with the issuance of the evaluation technical report *[ETR]*. The certification procedure has been conducted in accordance with the provisions of the EUCC as described in Commission implementing regulation (EU) 2024/482 of 31 January 2024, amended by (EU) 2024/3144 of 18 December 2024

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Huawei ATN Series Routers, version V800R022C00SPC600, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements.

Consumers of the Huawei ATN Series Routers, version V800R022C00SPC600 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

As per the *[ST]* conformance claim rationale, all the assumptions defined in the *[ST]* are taken with no exceptions. See section 2.4 for details.

The evaluation concluded that there are no special configuration requirements for the TOE besides the requirements defined in the user guidance. All users shall read these requirements and install the TOE in the operational environment accordingly.

The summary of the threats and security policies which *[ST]* defines:

- The Threats that are presented in Section 3.2 of *[ST]* include the threats addressed by the TOE and the IT. The assumed level of expertise of the attacker for all identified threats is Basic
- One Organizational Security Policy (OSPs) has been defined for this TOE

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 “Flaw Reporting Procedures”. This assurance level is recognised by article 52 of [CSA] as ‘substantial’

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CC:2022, Revision 1 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1 *[CC]* (Parts 1, 2, 3, 4, 5).

TrustCB B.V., as Certification Assessment Body licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities, declares that the product will be listed on the ENISA EU Cybersecurity Certificates list and that the evaluation meets all the conditions for international recognition of Common Criteria Certificates. Note that the certification results apply only to the specific version of the product as evaluated.

---

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the ICT product Huawei ATN Series Routers, version V800R022C00SPC600 from Huawei Technologies Co., Ltd located in Shenzhen, People's Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	ATN 910C-M	n/a
	ATN 910C-K	n/a
	ATN 910D-B	n/a
Software	Huawei ATN Series Router Software	V800R022C00SPC600

To ensure secure usage a set of guidance documents is provided, together with the Huawei ATN Series Routers, version V800R022C00SPC600. For details, see section 2.6 of this report, “Supplementary Cybersecurity Information.

The name and contact information provided for the holder of the issued Certificate associated with this Certification Report are as follows:

Organisation name:	Huawei Technologies Co., Ltd.
Address:	Administration Building, Headquarters of Huawei Technologies Co., Ltd., Bantian, Longgang District, Shenzhen, 518129, People’s Republic of China
Certified product contact	support@huawei.com
Website link for supplementary cybersecurity information associated with the TOE, in accordance with Article 55 of [EU-EUCC]	https://carrier.huawei.com/en/products/fixed-network/data-communication/router/atn1

2.2 Security Services

The major security features provided by the TOE are summarised as follows:

- Security audit
  - The log module of the host software records operations on a device and events that occur to a device. The recorded operations and events are log messages. Log messages provide evidence for diagnosing and maintaining a system. Log messages reflect the operating status of a device and are used to analyze the conditions of a network and to find out the causes of network failure or faults.
  - Key elements of log messages include timestamp, host name, Huawei identity, version, module name, severity, brief description, etc.
- Cryptographic support
  - The TOE provides cryptography in support of secure connections that includes remote administrative management.
- Identification and authentication

- The authentication functionality provides validation by user's account name and password. Public key authentication is supported for SSH users. Detailed functionalities, for example max idle-timeout period, max log-in attempts, UI lock, user kick out, can be applied by administrator

- Secure Management
  - The TOE restricts the ability to determine the behaviour of and modify the behaviour of the functions transmission of audit data to the security administrator. Only the security administrator can manage the cryptographic keys. Only the security administrator has the right of opening/closing the security services and creation/deletion/modification of the user accounts.
- Protection of the TSF
  - The TOE protects the pre-shared keys, symmetric keys, and private keys from reading them by an unauthorized entity. The TOE stores the users or administrator passwords in non-plaintext form preventing them from reading. The TOE verifies the packet before their installation and uses the digital signature.
- TOE access through user authentication
  - The TOE provides communication security by implementing SSH protocol.
  - To protect the TOE from eavesdrop and to ensure data transmission security and confidentiality, SSH implements:
    - authentication by password or by public-key;
    - AES encryption algorithms;
    - secure cryptographic key exchange;
    - Besides default TCP port 22, manually specifying a listening port is also implemented since it can effectively reduce attacks.
- Trusted path and channels for device authentication
  - The TOE supports the trusted connections using TLS for the communication with the audit server. The TOE protects communications between the TOE and all authorized remote administrators with SSH.

2.3 Vulnerability handling and Assurance Continuity Policies

The following vulnerability policy has been identified as applicable to the Huawei ATN Series Routers, version V800R022C00SPC600

Document reference: Huawei ATN Series Routers Flaw Remediation, Version 1.1

This is a new product certification. An assurance continuity policy was not provided.

2.4 Assumptions and Clarification of Scope

2.4.1 Assumptions

The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see 4.2 of the *[ST]*.

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE and its configuration in the environment to fulfil all Assumptions described in the [ST]. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

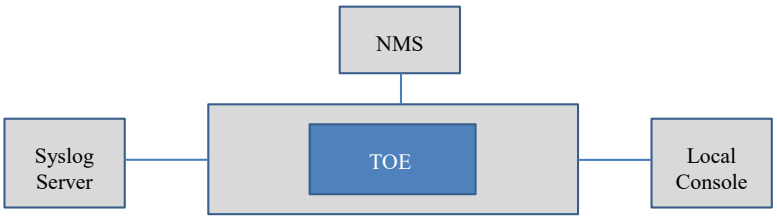
2.4.2 Clarification of scope

Considering all Assumptions above, the evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.5 Architectural Information

The Huawei ATN Series Routers TOE are used to satisfy the requirements for networks of various scales. They are deployed at the edge of MANs or at access sites that process heavy traffic to implement multi-service access.

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



The TOE hardware is identified as the following: ATN 910C-M, ATN 910C-K and ATN 910D-B which all have fixed physical interfaces. TSF relevant functions depend on software implementation.

2.6 Supplementary Cybersecurity Information

The contact information of the Huawei Technologies Co., Ltd was provided as support@huawei.com

The following website link was provided for Huawei ATN Series Routers, version V800R022C00SPC600 supplementary cybersecurity information as referred to in Article 55 of Regulation (EU) 2019/881:

https://carrier.huawei.com/en/products/fixed-network/data-communication/router/atn1

A “Learn more” link in the Product Supplementary Cybersecurity Information (EUCC) section of this page provides further details and links for:

- Guidelines to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Huawei ATN Series Routers, version V800R022C00SPC600.
- The period during which the Huawei ATN Series Routers, version V800R022C00SPC600 security support will be offered to end users, in particular as regards the availability of cybersecurity related updates, is stated as aligned with the validity of the EUCC certificate (5 years).
- Contact information and accepted method for receiving vulnerability information from end users and security researchers for the Huawei ATN Series Routers, version V800R022C00SPC600.
- the online repository listing publicly disclosed vulnerabilities related to the Huawei ATN Series Routers, version V800R022C00SPC600 and to any relevant cybersecurity advisories.

The following documentation, guidance and recommendations, is provided with the product by the developer to the customer to assist end users with the secure configuration, installation, deployment, operation and maintenance of the Huawei ATN Series Routers, version V800R022C00SPC600:

Identifier	Version
Huawei ATN Series Routers Operational User Guidance	1.2
Huawei ATN Series Routers Preparative Procedures	1.3
ATN 980C, 980B, 950D, 950C, 950B, 910C, 910D, 905 V800R022C00SPC600 Upgrade Guide	1.1
ATN 980C, 980B, 950D, 950C, 950B, 910D 910C and 905 V800R022C00 Product Documentation	1.0

2.7 Lifecycle Management processes and production facilities

Not applicable to this evaluation,

2.8 ICT Product Testing

2.8.1 Identification of CAB and ITSEF

TrustCB is the Certification Assessment Body, licensed by the Dutch Authority for Digital Infrastructure (RDI) for EUCC high certification activities.

TrustCB point of contact: EUCC@trustcb.com

Testing was performed by following ITSEF: SGS Brightsight B.V.

2.8.2 Identification of used assurance components

The assurance components used in the product testing were:

- **EAL 2 augmented with ALC_FLR.2**

as defined by, and detailed in, *[CC]* and *[CEM]*.

2.8.3 EUCC State of the Art documents and Protect Profiles

EUCC state-of-the-art documents *[SotA Documents]* were applied as referenced in the Bibliography.

No conformance to any production profile was claimed in this evaluation.

2.8.4 Testing approach and depth

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

For the testing performed by the evaluators, the developer provided samples of the TOE and host hardware. The evaluators performed defined tests from the source documentation used to derive the ST. During the evaluator analysis phase, no additional independent tests were identified as required to assess the assurance package.

2.8.5 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination several potential vulnerabilities were identified.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also, during this examination several potential vulnerabilities were identified.

- Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.

A judgment was made on whether potential vulnerabilities were exploitable. It was concluded that some potential vulnerabilities were not applicable or were covered by guidance. When a potential vulnerability was deemed feasible to be exploited, a penetration test was defined. The evaluator also executed a number of tests using scanning tools to verify if any potential vulnerabilities could impact any of the services running on the TOE in the evaluated configuration.

2.8.6 Test configuration

The TOE sample used for the majority of the testing was the Huawei ATN Series Router Software V800R022C00SPC600 running on hardware ATN 910-K. One test was performed on ATN 910C-M

There are different hardware versions supported by the TOE, however the difference between the various versions is the number of the same type of interfaces each offers. Therefore, the evaluation concluded that the testing of the TOE was considered valid for all hardware versions.

2.8.7 Test results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.8.8 Reused Evaluation Results

This was a new certification under EUCC however documentary evaluation results of an earlier version of the TOE certified under the Netherlands Scheme for Certification in the area of IT security (NSCIB-CC-23-0653316-CR) have been partially reused. Vulnerability analysis and penetration testing has been renewed

2.8.9 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei ATN Series Routers, version V800R022C00SPC600.

2.9 Results of the evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report, other evaluator documents and developer documentation *[DEV_DOCS]*.

The verdict of each claimed assurance requirement is "**Pass**".

2.9.1 Assessment against each assurance requirement

ASE

ASE	
ST introduction	ASE_INT.1
Conformance claims	ASE_CCL.1
Security problem definition	ASE_SPD.1

Security objectives	ASE_OBJ.2
Extended components definition	ASE_ECD.1
Security requirements	ASE.REQ.2
TOE summary specification	ASE.TSS.1
Consistency of Composite product ST	ASE.COMP.1

The findings are well-documented and internally consistent, demonstrating a thorough understanding of the Security Target *[ST]* and its components. The TOE introduction, conformance claim, security problems, security objectives, security requirements, TOE summary specification are appropriately addressed, and the TOE description is accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements of according EAL2 augmented with ALC_FLR.2

ADV

ADV	
Security architecture	ADV_ARC.1
Functional specification	ADV_FSP.2
TOE Design	ADV_TDS.1

The evaluation has demonstrated that the developer's evidence meets ADV specified requirements. The TOE model is complete, clearly showing all interfaces (TSFI/non-TSFI), user roles, and relations, with explanations on completeness and tracing requirements met. The subsystem/module level model is sensible, useful, and shows TSFIs and subsystem/module decomposition. The security architecture is thoroughly explained, design compliance rationale is complete and coherent, and necessary evidence is extracted per alternative approach. The evaluator confirmed why the TSF is well-structured. SFRs were inspected, with findings mapped to the implementation representation in both evaluation meetings. Accordingly, the ADV activities meet the assurance requirements for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

AGD

AGD	
Operational user guidance	AGD_OPE.1
Preparative procedures	AGD_PRE.1

The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure acceptance, installation, configuration, and operation of the TOE within its intended environment by its user roles. The guidance effectively helps prevent common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

ALC

ALC	
CM capabilities	ALC_CMC.2
CM Scope	ALC_CMS.2
Delivery	ALC_DEL.1
Flaw remediation	ALC_FLR.2

The evaluation has demonstrated that the developer's evidence meets ALC specified. The CI-list was comprehensive and uniquely identified all configuration items, with clear identification of the developer. The CM documentation effectively described unique identification methods, a CM plan for development, procedures for accepting modified or new CIs, and the CM system was operated in

accordance with the CM plan to maintain all configuration items by automated means. Delivery procedures were well-documented, ensuring security during TOE distribution. Flaw remediation procedures were comprehensive, including methods for receiving reports, tracking flaws, providing corrective actions, and updating users. Accordingly, the ALC activities satisfy the assurance requirements for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

ATE

ATE	
Coverage	ATE_COV.1
Functional tests	ATE_FUN.1
Independent testing	ATE_IND.2

The evaluation has demonstrated that the developer's evidence for ATE requirements meets all specified requirements. The testing approach used by the developer effectively covered the TSFIs. The developer's rationale for testing all TSFIs was presented and verified. For the evaluator's independent testing, the overall approach for test selection and independent test plan were clearly outlined. Repeated and independent tests were undertaken directly by the evaluators. The evaluator's testing results showed that all sampled tests were passed. Accordingly, the ATE activities satisfy the assurance requirements for EAL2 augmented with ALC_FLR.2, with no issues or deviations identified.

AVA

AVA	
Vulnerability analysis	AVA_VAN.2

Potential vulnerabilities were identified by the evaluator through conducting public domain vulnerability searches, SFR design analysis, applying known hardware and software vulnerability categories and use of scanning tools. The evaluator assessed the potential vulnerabilities and devised and executed testing for those that were judged feasible. Additionally, the evaluator re-executed a number of tests using scanning tools to verify if any new potential vulnerabilities could impact any of the services running on the TOE in the evaluated configuration.

Consequently, the AVA activities were performed in full compliance with the assurance requirements EAL2 augmented with ALC_FLR.2, providing a substantial level of confidence in the TOE's resistance to exploitation.

2.9.2 Overall result of evaluation

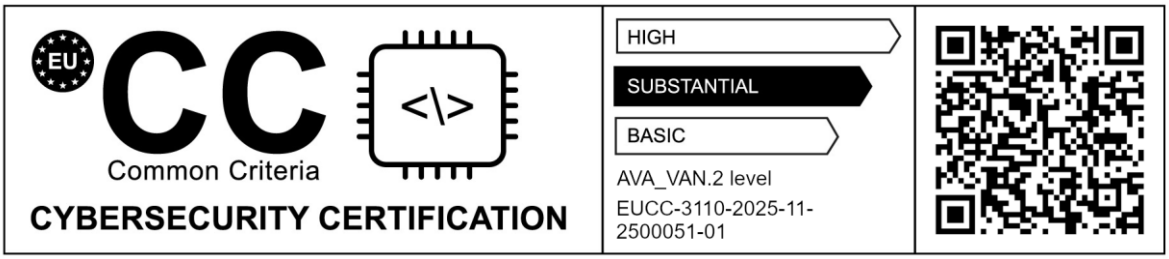
Based on the above evaluation results the evaluation lab concluded the Huawei ATN Series Routers, version V800R022C00SPC600, to be **CC:2022 revision 1 Part 2 extended, CC:2022 revision 1 Part 3 conformant**, at an assurance level recognised by article 52 of [CSA] as 'substantial', and to meet the requirements of **EAL 2 augmented ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Certificate information and scheme label

A Certificate has been issued recognising this evaluation result as follows:

Unique identifier: EUCC-3110-2025-11-2500051-01

Date of issuance: 14-11-2025 and with a validity period of **5 years**.



2.11 Comments/Recommendations

The user guidance as outlined in section 2.6 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details concerning the resistance against certain attacks.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. For the evolution of attack methods and techniques to be covered, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

3 Security Target

The Huawei ATN Series Routers Security Target, Version 2.5, 14 July 2025 *[ST]* is included here by reference.

This *[ST]* is summarised in the *[ETR]* as follows:

The Huawei ATN Series Routers TOE are used to satisfy the requirements for networks of various scales. They are deployed at the edge of MANs or at access sites that process heavy traffic to implement multi-service access.

Section 1.2 of *[ST]* describes the evaluated IT product. The security functionality of the evaluated IC product is represented by the implementation of the selected components of *[CC]* (Part 2) and are listed in section 6 of the *[ST]*, TOE Security Functional Requirements.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the *[CC]* or *[CEM]*:

EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EUCC	European Cybersecurity Certification Scheme *[EU-EUCC]*, created under the Cybersecurity Act *[EU-CSA]* and detailed in Commission Implementing Regulation (EU) 2024/482
IT	Information and communication technologies product as defined by *[EUCC]*
ITSEF	IT Security Evaluation Facility
OS	Operating System
SotA	EUCC State-of-the-Art document
TOE	Target of Evaluation; the object of the certification activity described by this report

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report.

[CC]	Common Criteria for Information Technology Security Evaluation, CC:2022 Parts 1, 2, 3, 4 and 4, Revision 1, November 2022
[CEM]	Common Methodology for Information Technology Security Evaluation, CEM:2022 Revision 1, November 2022
[ETR]	Evaluation Technical Report Huawei ATN Series Routers V800R022C00SPC600 – EAL2+, 25-RPT-866, Version 2.0, 10 October 2025
[EU-CSA]	REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
[EU-EUCC]	COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)
[ST]	Huawei ATN Series Routers Security Target, Version 2.5, 14 July 2025

(This is the end of this report.)