SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-088 CR Certification Report

Issue 1.0 25 November 2016

Huawei S Series Ethernet Switches V200R008C00SPC500

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

Certification Statement

Huawei Technology Co. Ltd. Huawei S Series Ethernet Switches is a series of switches that provides high-end networking capacities for telecom and enterprise core networks.

Huawei S Series Ethernet Switches version V200R008C00SPC500 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Arne Høye Rage Certifier Arne H. Rage
Quality Assurance	Kjartan Jæger Kvassnes Quality Assurance
Approved	Kristian Bae Head of SERTIT
Date approved	25 November 2016

1 Abbreviations

ACL	Access Control List
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MCU	Main Control Unit
MPU	Main Processing Unit
POC	Point of Contact
QP	Qualified Participant
RMT	Remote Maintenance Terminal
SERTIT	Norwegian Certification Authority for IT Security
SFU	Switching Fabric Unit
SoF	Strength of Function
SPM	Security Policy Model
SPU	Service Process Unit
SRU	Switch Router Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VRP	Versatile Routing Platform

2 References

[1] Security Target, Huawei Technology Co. Ltd., Huawei S Series Ethernet Switches V200R008 Security Target, version 1.5, 26 May 2016.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL3+ Evaluation of Huawei S Series Ethernet Switches V200R008C00, v2.0, 2016-11-09.

[8] CC Huawei S Series Ethernet Switches V200R008 - AGD_PRE, version 0.6, 2016-10-21

[9] CC Huawei S Series Ethernet Switches V200R008 - AGD_OPE, version 0.5, 2016-10-21.

[10] S2350&S5300&S6320 Series Ethernet Switches V200R008(C00&C10) Product Documentation, version 03, December 10th, 2015.

[11] S2750EI&S5700&S6720 Series Ethernet Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[12] S7700&S9700 Series Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[13] S9300&S9300E Series Switches V200R008(C00&C10) Product Documentation version 04, March 10th, 2015.

[14] S12700 Series Agile Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[15] E600 V200R008C00 Product Documentation, version 02, October 23rd, 2015.

3 Executive Summary

3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei S Series Ethernet Switches version V200R008C00SPC500 to the Sponsor, Huawei Technology Co. Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

3.2 Evaluated Product

The version of the product evaluated was Huawei S Series Ethernet Switches and version V200R008C00SPC500.

These products are also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technology Co. Ltd.

Huawei S Series Ethernet Switches V200R008, the TOE, provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware and software.

At the core of each switch is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include different interfaces with according access levels for administrators; 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.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

3.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.2.1 and 1.4.2.2.

3.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

3.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 3, augmented by

ALC_FLR.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

3.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

3.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

3.8 Threats Countered

- **T.UnwantedL2NetworkTraffic**
  Unwanted L2 network traffic sent to the TOE will cause the MAC table gets updated dynamically by MAC learning function. This may due the MAC table overload.
  In the TOE Layer 2 switching network, loops on the network cause packets to be continuously duplicated and propagated in the loops, leading to the broadcast storm, which exhausts all the available bandwidth resources and renders the network unavailable.
- **T.UnwantedL3NetworkTraffic**
  Unwanted L3 network traffic sent to the TOE will not only cause the TOE's processing capacity for incoming network traffic is consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to the Control Plane.
  This may further cause the TOE to fail to respond to system control and security management operations. Routing information exchanged between the TOE and peer routes may also be affected due the traffic overload.
- **T.UnauthenticatedAccess**
  A user who is not an administrator gains access to the TOE.
- **T.UnauthorizedAccess**
  A user authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
- **T.Eavesdrop**
  An eavesdropper (remote attacker) is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and LMT/RMT.

3.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

3.11 Environmental Assumptions and Dependencies

It is assumed that the TOE (including any console attached, access of CF card) is protected against unauthorized physical access.

The environment is supposed to provide supporting mechanism to the TOE:

- A Radius server for external authentication/authorization decisions;
- Peer router(s) for the exchange of dynamic routing information;
- A remote entities (PCs) used for administration of the TOE.
- An SNMP Server used for collecting SNMP traps

It is assumed that the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the application (or, public) networks where the interfaces in the TOE are accessible.

The authorized administrators are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

3.12 IT Security Objectives

The following objectives must be met by the TOE:

- **O.Forwarding (all series except S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)**
  The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a configured route for the destination IP address of the packet, or corresponds with a MAC address for the destination MAC address of the packet. When TOE works as Layer 2 forwarding device, users should be isolated between VLANs. And TOE can find the loops in the network, and block certain interfaces to eliminate loops.
- **O.Forwarding (S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)**
  The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a MAC address for the destination MAC address of the packet. Users should be isolated between VLANs. And TOE can find the loops in the network, and block certain interfaces to eliminate loops.
- **O.Communication**
  The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.
- **O.Authorization**
  The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- **O.Authentication**
  The TOE must authenticate users of its user access.

- **O.Audit**
  The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.Resource**
  The TOE shall provide functionalities and management for assigning a priority (used as configured bandwidth), enforcing maximum quotas for bandwidth and MAC address table entries, to prevent internal collapse due to traffic overload .
- **O.Filter**
  The TOE shall provide ACL or packet filter to drop unwanted L2 or L3 network traffic.

3.13 Non-IT Security Objectives

- 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, SNMP Servers and Radius servers for obtaining authentication and authorization decisions.
- OE.Physical
  The TOE (i.e., the complete system including attached peripherals, such as a console, and CF card inserted in the Switch) shall be protected against unauthorized physical access.
- OE.NetworkSegregation
  The operational environment shall provide segregation by deploying the management interface in TOE into an independent local -network.
- OE.Person
  Personnel working as authorized administrators shall be carefully selected for trustworthyness and trained for proper operation of the TOE.

3.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.3 Action in case of possible audit data loss
- FCS_COP.1/AES Cryptographic operation
- FCS_COP.1/RSA Cryptographic operation
- FCS_COP.1/DHKeyExchange Cryptographic operation
- FCS_COP.1/HMAC-MD5SHA256 Cryptographic operation
- FCS_COP.1/MD5 Cryptographic operation
- FCS_CKM.1/AES Cryptographic key generation

- FCS_CKM.1/RSA Cryptographic key generation
- FCS_CKM.1/DHKey Cryptographic key generation
- FCS_CKM.4/RSA Cryptographic key destruction
- FCS_CKM.4/AES-DHKey Cryptographic key destruction
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_DAU.1 Basic Data Authentication (for all series except S23XX-EI,S53XX-LI/SI,S27XX-EI,S57XX-LI/SI,E6XX)
- FDP_DAU.1 Basic Data Authentication (for S23XX-EI/S53XX-LI/ S23XX-EI,S53XX-LI/SI,S27XX-EI,S57XX-LI/SI,E6XX)
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes (for all series except S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)
- FDP_IFF.1 Simple security attributes (for S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)
- FIA_AFL.1 Authentication failure handling (this does not apply to RADIUS authentication)
- FIA_ATD.1 User attribute definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User authentication before any action
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behavior
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps
- FPT_FLS.1 Fail secure
- FRU_PRS.1 Limited priority of service
- FRU_RSA.1 Maximum quotas
- FRU_FLT.1 Degraded fault tolerance
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path

3.15 Security Function Policy

The VRP is the control and management platform that runs on the SRU/MCU. The VRP supports IPv4/IPv6, and routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), calculates routes, generates forwarding tables, and delivers routing information to the LPU(s). The VRP includes Service Control Plane (SCP), System Manage Plane (SMP), General Control Plane (GCP) and other TSF, non-TSF sub-systems.

The OS is supplied for the commercial use of embedded real-time operating system, a driving system for the CPU, and provide the basis for the VRP system scheduling mechanism.

There is one difference between the software architecture of Box Switch and the Chassis Switch: in Box Switches the LPU and VP are done in SW, but in Chassis Switches, this is done in HW.

Note that for the S23xx-EI/S53xx-LI and S27xx-EI/S57xx-LI (who do not support L3 forwarding), the S53xx-SI, E6xx and S57xx-SI (who only support static routing), the software architecture is identical, but the commands required to support non-existing functionality will simply return error messages.

3.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 01-11-2016. SERTIT then produced this Certification Report.

3.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

4 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 3 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_FLR.2	Flaw reporting procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

4.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

4.2 Delivery

The TOE delivery procedures are outlined for the consumer in [8]. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

4.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the Preparative Procedures document[8] provided by the developer, which describes all necessary steps to configure the TOE in the certified configuration. The Operational Guidance document[9] further shows what measures should be taken to ensure that the operational environment meets the objectives described in Section 3.13. Finally, these documents may refer to the product manuals ([10][11][12][13][14][15]), which provide a detailed list of instructions and commands.

The above documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner. The readers are recommended to note the following:

- Use only one password for different items (like admin password, bgp md5 authentication strings, ospf authentication string, snmp authentication string) is very dangerous, configure different password is the better way. Using the same authentication strings across the entire network is also easier to be hacked.
- During startup it is possible on the console interface to select the option to boot up from a remote FTP/TFTP server. This facility is only to be used for emergencies and make sure that the network(s) between operator and the FTP/TFTP-server are secure, as well as the FTP/TFTP-server itself.

4.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

4.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The TOE are substantially similar to other router/switches on the market. This technology is well-established. The technology and possible vulnerabilities are described in a series of public documents.

The evaluators assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found but only two turned out to be possibly exploitable. The developer has updated the guidance to enhance the secure configuration of the TOE, and as a result this issue has become moot.

4.6 Developer's Tests

The Developer Test Plan consists of 11 different categories, each containing between 1 and 13 tests. The categories are based on major groupings of security functionality, and in combination cover all SFRs and TSFIs.

4.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing because, although the developer's testing was extensive, some additional assurance could be gained by additional testing.

For independent testing, the evaluator has made a sample of one test of each category, with one exception, as that category has only one test and this test was sufficiently repeated later on.

5 Evaluation Outcome

5.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Huawei S Series Ethernet Switches version V200R008C00SPC500 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

5.2 Recommendations

Prospective consumers of Huawei S Series Ethernet Switches version V200R008C00SPC500 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

The administrators should note that the correctness of the configuration files is not checked by the TOE, and therefore the administrators must follow the instructions given in the guidance, ensuring the correctness of the configuration files themselves before applying them to the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of the Huawei S2300 series, S2700 series, S5700 series, S5300 series, S6700 series, S6300 series, E600 series, S5720 series, S6720 series, S6320 series, S12700 series, S7700 series, S9300 series, and S9700 series of switches, running VRP V200R008C00.

There are some minor security differences between the various series, i.e., not all series support all functionality:

- The S23xx-EI/S53xx-LI and S27XX-EI/S57XX-LI do not support L3 forwarding.
- The S53xx-SI, S57xx-SI and E6XX only support static routing and no OSPF/BGP.

Hardware

Model Types	Typical System Configuration and Physical Parameters		
S5300	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 5300LI: 1GHZ	-
	SDRAM	5300LI: 256MB	-
	Flash	5300LI: 200MB	-
	CF card	-	-
	Switching capacity	5300-28P-LI: 56Gbps 5300-52P-LI: 104Gbps 5300-28X-LI: 128Gbps 5300-10P-LI: 26Gbps (bidirectional)	-
	Forwarding capacity	5300-28P-LI: 41.66Mpps 5300-52P-LI: 77.4Mpps 5300-28X-LI: 95.2Mpps 5300-10P-LI: 15Mpps	-
S5320	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: S5320SI: 800MHz S5320EI: 1GHz	-
	SDRAM	S5320SI: 512MB S5320EI: 2GB	-
	Flash	S5320SI: 240MB S5320EI: 340MB	-
	CF card	-	-

	Switching capacity	S5320-28P-SI: 168Gbps S5320-28X-SI: 168Gbps S5320-52P-SI: 336Gbps S5320-52X-SI: 336Gbps S5320-32P-EI: 220Gbps S5320-32X-EI: 220Gbps S5320-36C-EI: 220Gbps S5320-50X-EI: 260Gbps S5320-52P-EI: 260Gbps S5320-52X-EI: 260Gbps S5320-56C-EI: 260Gbps (bidirectional)	-
	Forwarding capacity	S5320-28P-SI: 41.7Mpps S5320-28X-SI: 95.2Mpps S5320-52P-SI: 77.4Mpps S5320-52X-SI: 131Mpps S5320-32P-EI: 47.6Mpps S5320-36PC-EI:77.4Mpps S5320-32X-EI: 101.2Mpps S5320-36C-EI: 131Mpps S5320-50X-EI: 128Mpps S5320-52P-EI: 77.4Mpps S5320-52X-EI: 131Mpps S5320-56C-EI: 160.7Mpps S5320-56PC-EI:107.1Mpps	-
S2300	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 800MHz	-
	SDRAM	256 MB	-
	Flash	200 MB	-
	CF card	-	-
	Switching capacity	S2350-20TP: 11.2Gbit/s S2350-28TP: 12.8Gbit/s (bidirectional)	-
	Forwarding capacity	S2350-20TP: 8.33Mpps S2350-28TP: 9.53Mpps	-
S6320	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: S6320EI: 1.2GHz	-
	SDRAM	S6320EI: 2GB	-

	Flash	S6320EI: 240MB	-
	CF card	-	-
	Switching capacity	S6320EI: 1.44Tbps (bidirectional)	-
	Forwarding capacity	S6320-30C-EI: 714.2Mpps S6320-54C-EI: 1071.4Mpps	-
S5700	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 5700LI: 1GHZ	-
	SDRAM	5700LI: 256MB	-
	Flash	5700LI: 200MB	-
	CF card	-	-
	Switching capacity	5700-28P-LI: 56Gbps 5700-52P-LI: 104Gbps 5700-28X-LI: 128Gbps 5700-52X-LI: 256Gbps 5700-10P-LI: 26Gbps (bidirectional)	-
	Forwarding capacity	5700-28P-LI: 41.66Mpps 5700-52P-LI: 77.4Mpps 5700-28X-LI: 95.2Mpps 5700-52X-LI: 132Mpps 5700-10P-LI: 15Mpps S5710-108C-HI: 504Mpps	-
S5720	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: S5720SI: 800MHz S5720EI: 1GHz S5720HI: 1.2GHz	-
	SDRAM	S5720SI: 512MB S5720EI: 2GB S5720HI: 4GB	-
	Flash	S5720SI: 240MB S5720EI: 340MB S5720HI: 400MB	-
	CF card	-	-

	Switching capacity	S5720SI: 168Gbps S5720-52P-SI: 336Gbps S5720-52X-SI: 336Gbps S5720-32P-EI: 220Gbps S5720-32X-EI: 220Gbps S5720-36C-EI: 220Gbps S5720-50X-EI: 260Gbps S5720-52X-EI: 260Gbps S5720-56C-EI: 260Gbps S5720HI: 265Gbps (bidirectional)	-
	Forwarding capacity	S5720-28P-SI: 41.7Mpps S5720-28X-SI: 95.2Mpps S5720-52P-SI: 77.4Mpps S5720-52X-SI: 131Mpps S5720-32P-EI: 47.6Mpps S5720-36PC-EI: 77.4Mpps S5720-52P-EI: 77.4Mpps S5720-32X-EI: 101.2Mpps S5720-56PC-EI: 107.1Mpps S5720-50X-EI: 128Mpps S5720-36C-EI: 131Mpps S5720-52X-EI: 131Mpps S5720-56C-EI: 160.7Mpps S5720-32C-HI: 166.7Mpps S5720-56C-HI: 190.5Mpps	-
S2700	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 800MHz	-
	SDRAM	256 MB	-
	Flash	240 MB	-
	CF card	-	-
	Switching capacity	S2750-20TP: 11.2Gbps S2750-28TP: 12.8Gbps (bidirectional)	-
	Forwarding capacity	S2750-20TP: 8.33Mpps S2750-28TP: 9.52Mpps	-
S6720	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: S6720HI: 1.2GHz	-
	SDRAM	S6720HI: 2GB	-
	Flash	S6720HI: 240MB	-

	CF card	-	-
	Switching capacity	S6720HI: 1.44Tbps (bidirectional)	-
	Forwarding capacity	S6720-30C-EI: 714.2Mpps S6720-54C-EI: 1071.4Mpps	-
S9303 S7703	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 500 MHz	-
	SDRAM	512 MB	
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	1.92 Tbps	-
	Forwarding capacity	1440 Mpps	-
	Max MCU slots	2	MCUs work in 1:1 redundancy.
	Max LPU slots	3	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 40*10Gbps 2*40Gbps 2*100Gbps/s	-
S9306 S7706	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.5 GHz	-
	SDRAM	4 GB	
	CF card	-	
	Switching capacity	3.84 Tbps	-
	Forwarding capacity	2880 Mpps	-

	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	6	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 40*10Gbps 2*40Gbps 2*100Gbps/s	-
S9312 S7712	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.5 GHz	-
	SDRAM	4 GB	
	CF card	-	
	Switching capacity	3.84 Tbps	-
	Forwarding capacity	2880 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	12	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 40*10Gbps 2*40Gbps 2*100Gbps/s	-
S9303E S9703	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 500 MHz	-
	SDRAM	512 MB	
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	2.88 Tbps	-
	Forwarding	2160 Mpps	-

	capacity		
	Max SRU slots	2	MCUs work in 1:1 redundancy.
	Max LPU slots	3	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 48*10Gbps 8*40Gbps 2*100Gbps/s	-
S9306E S9706	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.2G MHz	-
	SDRAM	2GB	
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	6.72 Tbps	-
	Forwarding capacity	2880 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	6	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 48*10Gbps 8*40Gbps 2*100Gbps/s	-
S9312E S9712	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.2G MHz	-
	SDRAM	2GB	
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device

			for storing data files. There are two CF cards on the SRU.
	Switching capacity	8.64 Tbps	-
	Forwarding capacity	3840 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	12	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 48*10Gbps 8*40Gbps 2*100Gbps/s	-
S12700	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 1.5G MHz	-
	SDRAM	4GB	
	CF card	-	-
	Switching capacity	S12704: 4.88 Tbps S12708: 12.32 Tbps S12712: 17.44 Tbps	-
	Forwarding capacity	S12704: 3120 Mpps S12708: 6240 Mpps S12712: 9120 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	S12704: 4 S12708: 8 S12712: 12	-
	Maximum interface rate per LPU	48*100Mbps 48*1Gbps 48*10Gbps 8*40Gbps 2*100Gbps/s	-
E600	**Item**	**Typical Configuration**	**Remark**
	Processing unit	Main frequency: 800 MHz	-
	SDRAM	E600: 512MB	-
	Flash	E600: 240MB	-

	CF card	-	-
	Switching capacity	E628: 168Gbps E628-X: 168Gbps E652: 336Gbps E652-X: 336Gbps (bidirectional)	-
	Forwarding capacity	E628: 41.664Mpps E628-X: 95.232Mpps E652: 77.376Mpps E652-X: 130.944Mpps	-

Table 1: Hardware Scope

Software

Type	Name	Version
Software	Product software	V200R008C00SPC500
	VRP	Version 5 Release 16
	VxWorks (S2700\S5700\S7700\S9700\S2300\S5300\S9300)	5.5
	Windriver (Linux kernel 2.6.34) (S5720\S6720\S5320\S6320\E600\S12700)	4.3

Table 2: Software Scope

Guidance

Type	Name	Version
Guidance	S2350&S5300&S6320 V200R008 Product Documentation	03
	S2750EI&S5700&S6720 V200R008C00 Product Documentation	04
	S7700&S9700 V200R008C00 Product Documentation	02
	S9300&S9300E V200R008 Product Documentation	02
	S12700 V200R008C00 Product Documentation	02
	E600 V200R008C00 Product Documentation	02
	CC Huawei S Series Ethernet Switches V200R008 - AGD_OPE	V0.5
	CC Huawei S Series Ethernet Switches V200R008 - AGD_PRE	V0.6

Table 3: Guidance Scope

TOE Documentation

The supporting guidance documents evaluated were:

[a] CC Huawei S Series Ethernet Switches V200R008 - AGD_PRE, version 0.6, 2016-10-21.

[b] CC Huawei S Series Ethernet Switches V200R008 - AGD_OPE, version 0.5, 2016-10-21

[c] S2350&S5300&S6320 Series Ethernet Switches V200R008(C00&C10) Product Documentation, version 03, December 10th, 2015.

[d] S2750EI&S5700&S6720 Series Ethernet Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[e] S7700&S9700 Series Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[f] S9300&S9300E Series Switches V200R008(C00&C10) Product Documentation version 04, March 10th, 2015.

[g] S12700 Series Agile Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015.

[h] E600 V200R008C00 Product Documentation, version 02, October 23rd, 2015.

Further discussion of the supporting guidance material is given in Section 4.3 "Installation and Guidance Documentation".

TOE Configuration

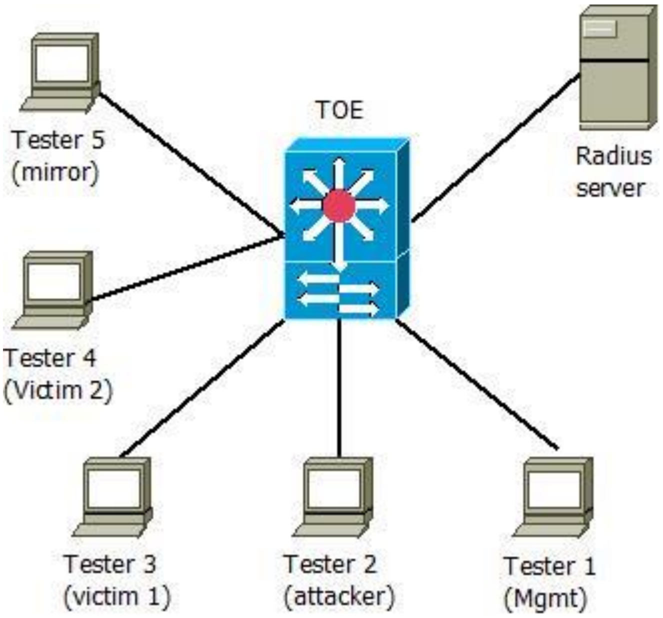
The following configuration was used for testing:

ITEM	IDENTIFIER
HARDWARE	One of the hardware models listed in section TOE Identification
SOFTWARE	Product software version V200R008C00SPC500, VRP V500R016, VxWorks 5.5 / WRLinux 4.3 configured according to [8].

MANUALS	CC Huawei S Series Ethernet Switches V200R008 - AGD_PRE, version 0.6, 2016-10-21. CC Huawei S Series Ethernet Switches V200R008 - AGD_OPE, version 0.5, 2016-10-21 S2350&S5300&S6320 Series Ethernet Switches V200R008(C00&C10) Product Documentation, version 03, December 10th, 2015. S2750EI&S5700&S6720 Series Ethernet Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015. S7700&S9700 Series Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015. S9300&S9300E Series Switches V200R008(C00&C10) Product Documentation version 04, March 10th, 2015. S12700 Series Agile Switches V200R008C00 Product Documentation, version 02, October 23rd, 2015. E600 V200R008C00 Product Documentation, version 02, October 23rd, 2015.

Environmental Configuration

The TOE is tested in the following set-up:


TOE
Tester 5
(mirror)
Radius
server
Tester 4
(Victim 2)
Tester 3
(victim 1)
Tester 2
(attacker)
Tester 1
(Mgmt)