SERTIT

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

SERTIT-064 CR Certification Report

Issue 1.0 23 November 2015

Huawei FusionSphere v5

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 recognised under the terms of the CCRA May 23rd 2000. The recognition under CCRA is limited to EAL 4 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.

Contents

1 Certification Statement

Huawei Technology Co. Ltd. Fusionsphere is a a software system that can provide multiple VMs on industry standard x86-compatible hardware platforms (64-bit) and allows the management of these virtual machines (VMs).

Fusionsphere version v5 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has 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	Kjartan Kvassnes Certifier K Kvassnes
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Øystein Hole Head of SERTIT Øystein Hole
Date approved	23 November 2015

2 Abbreviations

ACL	Access Control List
AD	Activity Directory
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
CNA	Compute Node Agent
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
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
O&M	Operation and Management
OSS	Operating Support System
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SPM	Security Policy Model
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

TSP	TOE Security Policy
UVP	Universal Virtualization Platform
VDC	Virtual Data Center
VIF	Virtual Interface
VLAN	Virtual Local Area Network
VM	Virtual Machine
VRF	Virtual Router Function
VRM	Virtualization Resources Management

3 References

[1] Security Target, Huawei Technology Co. Ltd., version 1.0, 2015-06-30.

[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 the Huawei FusionSphere v5, version 2.0, 2015-09-11.

[8] FusionSphere Solution Documentation, V100R005C00

[9] FusionSphere Preparative Procedures, V100R005C00 Issue 02

[10] FusionSphere Operational User Guidance, V100R005C00 Issue 03

[11] FusionManager Product Documentation, V100R005C00

[12] FusionManager Tenant Guide, V100R005C00

[13] FusionManager Administrator Guide, V100R005C00

[14] FusionManager Software Installation Guide, V100R005C00

[15] FusionCompute Product Documentation, V100R005C00

[16] FusionCompute Security Guide, V100R005C00

[17] FusionCompute Configuration Management Guide, V100R005C00

[18] FusionStorage Product Documentation, V100R003C02

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Fusionsphere version v5 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.

4.2 Evaluated Product

The product evaluated was Fusionsphere version v5.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technology Co. Ltd.

Huawei FusionSphere is a software system that can provide multiple VMs on industry standard x86-compatible hardware platforms (64-bit) and allows the management of these virtual machines (VMs). It virtualizes hardware resources so that one physical server can function as multiple virtual servers. It consolidates existing workloads on servers and allows new applications and solutions to be deployed to improve server utilization and consolidation ratio.

Huawei FusionSphere provides a unified O&M portal for O&M engineers. O&M engineers can remotely access the FusionSphere system using a web browser and perform operations such as resource management, resource monitoring, and resource statistics reporting.

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

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.3 and 1.4.5

4.4 Protection Profile Conformance

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

4.5 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].

4.6 Security Policy

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

4.7 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.

4.8 Threats Countered

- T.NOIDENTIFY
  A user who is not a user of the TOE gains access to the TOE.

- T.NOAUTH
  A user of the TOE authorized to perform certain actions and access certain information gains access to function or information he is not authorized to access.

- T. EAVESDROP
  An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.

- T.VM_DOM_BYPASS
  A process running on one virtual machine might compromise the security of processes running on that and other virtual machines and its resources.

- T.HOST_DOM_BYPASS
  An individual may compromise the physical machine processes and resources, potentially affecting other VMs.

- T.VNETWORK_BYPASS
  An individual may access a virtual network belonging to VMs that do not belong to such individual.

4.9 Threats Countered by the TOE's environment

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

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

It is assumed the authorized administrators (including northbound interface users) are not careless, wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

It is assumed the OS users are trusted and will not attack the TOE.

It is assumed that the ETH interface of management and storage plane in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.

The FusionManager manages the NEs through the internal management network plane. It is assumed that the internal management network is secure and the NEs are trusted.

It is assumed that the TOE is protected against unauthorized physical access. Unauthorized users cannot gain access to these devices or components.

It is assumed the environment will provide reliable time stamps for the generation of audit records.

It is assumed that the OSs for FusionManager, FusionStorage Manager and VRM are trusted and the third party OSS is trusted.

4.12 IT Security Objectives

- O.Authentication
  The TOE must authenticate users before allowing them access to its management interface.

- O. Authorization
  The TOE shall allow different authorization levels to be assigned to administrators in order to restrict the functionality that is available to individual administrators.

- O. Communication
  The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.

- O.Audit
  The TOE must be able to generate and review audit records for

security-relevant events.

- O.VM_DOM_ISO
  The TOE must provide virtual machines with a domain of execution and resources protection from interference and tampering by other virtual machines running the same physical host.

- O.VNETWORK_ISO
  The TOE must maintain virtual networks used for VMs isolated from each other.

4.13 Non-IT Security Objectives

- OE.PHY_PROTECTION
  The operational environment shall protect the TOE against unauthorized physical access.

- OE.SEP_PHY_NETWORK
  The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.
  The operational environment shall ensure that the internal management network is secure and the NEs are trusted.

- OE.TRUST_WORTHY_USER Personnel working as authorized administrators (including northbound interface users) shall be carefully selected for trustworthiness and trained for proper operation of the TOE.

- OE.TIME_SRC
  The operational environment shall provide reliable time source.

- OE.OS_TRUSTED
  The operational environment shall ensure the OSs for FusionManager, FusionStorage Manager and VRM are trusted and the third party OSS is trusted and will not be used to attack the TOE.

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.2 Restricted 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

- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_IFC.1(1) Subset information flow control- VM Data
- FDP_IFF.1(1) Simple security attributes- VM Data
- FDP_IFC.1(2) Subset information flow control- VM Network
- FDP_IFF.1(2) Simple security attributes- VM Network
- FDP_RIP.1 Subset residual information protection
- FIA_AFL.1 Authentication failure handling
- 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 behaviour
- 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
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path
- FPT_ITT.1 Internal TOE TSF data transfer protection

4.15 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 Brightsight B.V Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 11 September 2015. SERTIT then produced this Certification Report.

4.16 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.

5 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.

5.1 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.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.4.3 and Preparative Procedures documents [9] provided by the developer. The Preparative procedures [9] and the Operational guidance [10] describe all necessary steps to configure the TOE in the certified configuration.

These 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 point:

- The TOE does not support the high availability (HA) configuration in the certified configuration. In the certified configuration the TOE only can work in standalone mode.

5.4 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.

5.5 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 major functionality of the TOE is to provide a virtualization solution and is based on the open source hypervisor, the XEN project. The vulnerabilities are well reviewed by the open source community. 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 and several of them turned out to be possibly exploitable. As a result the developer has to patch the TOE to mitigate the vulnerabilities, and updated the guidance to enhance the secure configuration of the TOE. As a result, the issues discovered become moot.

5.6 Developer's Tests

The Developer Test Plan consists of 8 different categories, each containing between 1 and 11 tests. The categories are based on major groupings of security functionality, and in combination cover all SFRs and TSFIs.

5.7 Evaluators' Tests

For independent testing it was decided to sample one test of each category to be repeated in his presence, thereby guaranteeing a good spread of these tests over the SFRs/TSFIs. The evaluator has also made sure that there is no overlap between these tests and the tests in the ATE IND, thereby maximizing coverage.

The evaluator also analyzed the Developer Test Plan to see where additional ATE tests could be performed, and tests selected 4 additional (see further):

All of these tests were performed at both the Huawei premises in Xi'An and at Brightsight during the period between 13th October 2014 to 30th June 2015.

6 Evaluation Outcome

6.1 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 Fusionsphere version v5 meets 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.

6.2 Recommendations

Prospective consumers of Fusionsphere version v5 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 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

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

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of the following software:

FusionCompute VRM	V100R005C00CP3002
FusionCompute CNA	V100R005C00CP3002
FusionCompute Tools	V100R005C00SPC300
FusionManager	V100R005C00SPC302
FusionStorage Manager	V100R003C02SPC301
FusionStorage Agent	V100R003C02SPC301

And the following guidance:

FusionSphere Solution Documentation	V100R005C00
FusionSphere Preparative Procedures Issue 02	V100R005C00
FusionSphere Operational User Guidance Issue 03	V100R005C00
FusionManager Product Documentation	V100R005C00
FusionManager Tenant Guide	V100R005C00
FusionManager Administrator Guide	V100R005C00
FusionManager Software Installation Guide	V100R005C00
FusionCompute Product Documentation	V100R005C00
FusionCompute Security Guide	V100R005C00
FusionCompute Configuration Management Guide	V100R005C00
FusionStorage Product Documentation	V100R003C02

TOE Documentation

The supporting guidance documents evaluated were:

[a] FusionSphere Solution Documentation, V100R005C00

[b] FusionSphere Preparative Procedures, V100R005C00 Issue 02

[c] FusionSphere Operational User Guidance, V100R005C00 Issue 03

[d] FusionManager Product Documentation, V100R005C00

[e] FusionManager Tenant Guide, V100R005C00

[f] FusionManager Administrator Guide, V100R005C00

[g] FusionManager Software Installation Guide, V100R005C00

[h] FusionCompute Product Documentation, V100R005C00

[i] FusionCompute Security Guide, V100R005C00

[j] FusionCompute Configuration Management Guide, V100R005C00

[k] FusionStorage Product Documentation, V100R003C02...

Further discussion of the supporting guidance material is given in Section 5.3 “Installation and Guidance Documentation”.

TOE Configuration

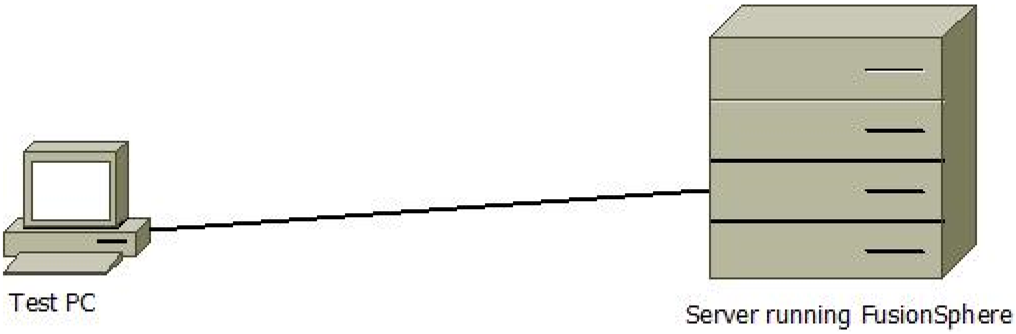
The following configuration was used for testing:

ITEM	IDENTIFIER
HARDWARE	N/A
SOFTWARE	All of the software listed in “TOE Identification” configured according to [b] and [c].
MANUAL	The appropriate guidance document in “TOE Documentation”

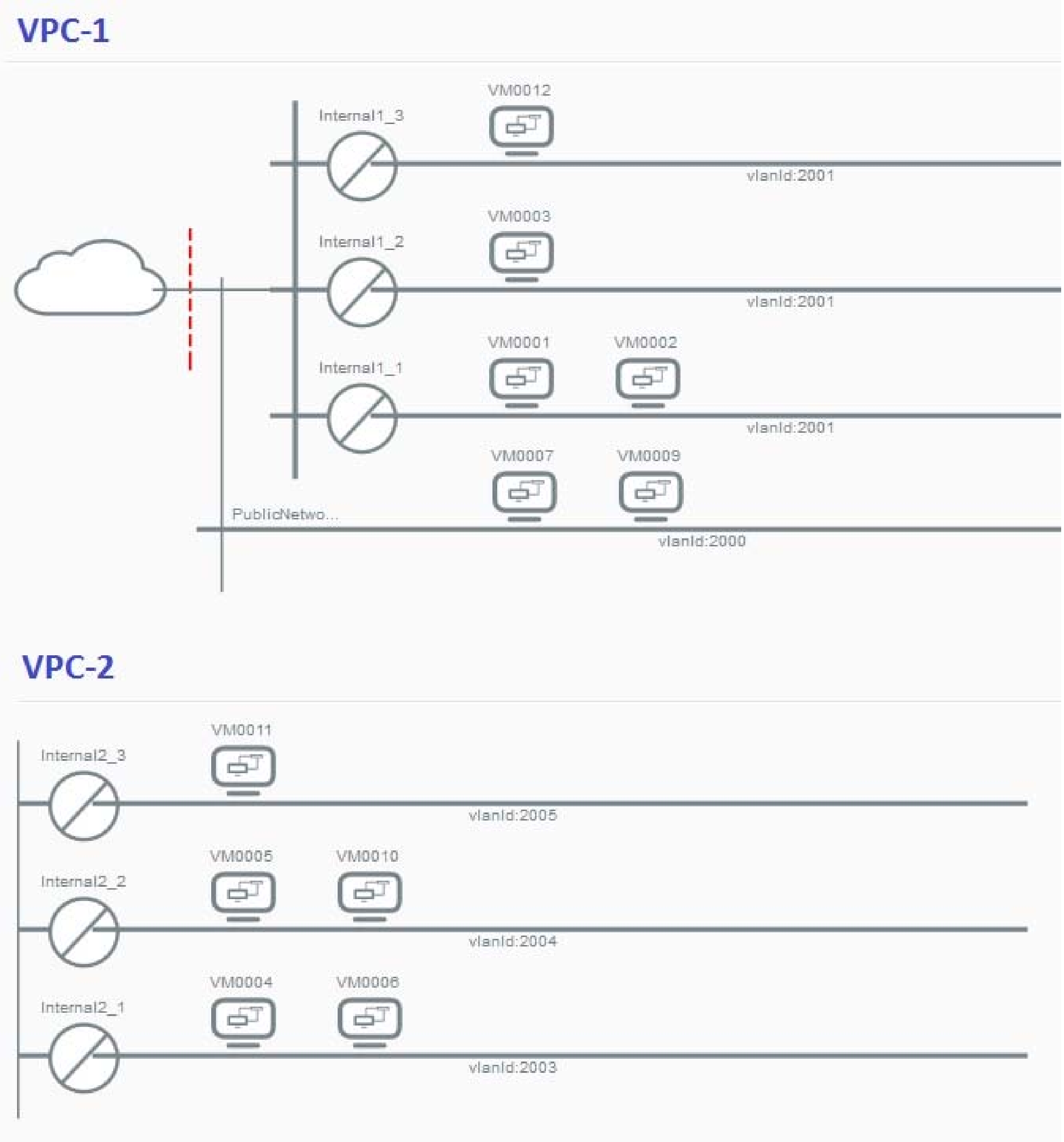
Environmental Configuration

The TOE is tested in the following test setups:

The following figure shows general setup for testing VM isolation and management interface:



The following network diagram describes the overall setup of the testing environment. Two Virtual Private Cloud (VPC) were created. This test setup is mainly to test the virtual network separation.


VPC-1
VM0012
Internal1_3
vlanId:2001
VM0003
Internal1_2
vlanId:2001
VM0001
VM0002
Internal1_1
vlanId:2001
VM0007
VM0009
PublicNetwo...
vlanId:2000
VPC-2
VM0011
Internal2_3
vlanId:2005
VM0005
VM0010
Internal2_2
vlanId:2004
VM0004
VM0006
Internal2_1
vlanId:2003