Certification Report

VMware vCloud Networking and Security 5.5.0a

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-228-CR
Version: 1.0
Date: 26 March 2014
Pagination: i to iii, 1 to 13

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility .

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 26 March 2014, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademark or registered trademark:

- VMware is a registered trademark or trademark of VMware, Inc.

TABLE OF CONTENTS

Executive Summary

VMware vCloud Networking and Security 5.5.0a (hereafter referred to as VCNS v5.5.0a), from VMware, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

VCNS v5.5.0a is a network virtualization and security product for protecting virtualized datacenters from network-based attacks, protecting data in transit between datacenters and preventing misuse of network services and protected information contained within the network. VCNS v5.5.0a includes virtual appliances and services essential for protecting virtual machines from attacks within/from the virtual and the physical environments. VCNS v5.5.0a can be configured through a web-based user interface, a vSphere Client plug-in, vCenter Server snap-in, a command line interface (CLI), and REST API.

VCNS v5.5.0a is comprised of a suite of networking and security virtual appliances built for VMware vSphere integration. VMware vCenter Server provides centralized management of VMware's ESXi. VMware ESXi and vCenter Server 3.5, 4.0, 4.1, and 5.0 have been Common Criteria evaluated. ESXi is a user-installable or OEM-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 26 February 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for VCNS v5.5.0a, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 *augmented* assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting.

Communications Security Establishment, as the CCS Certification Body, declares that the VCNS v5.5.0a evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is VMware vCloud Networking and Security 5.5.0a (hereafter referred to as VCNS v5.5.0a), from VMware, Inc..

2 TOE Description

VCNS v5.5.0a is a network virtualization and security product for protecting virtualized datacenters from network-based attacks, protecting data in transit between datacenters and preventing misuse of network services and protected information contained within the network. VCNS v5.5.0a includes virtual appliances and services essential for protecting virtual machines from attacks within/from the virtual and the physical environments. VCNS v5.5.0a can be configured through a web-based user interface, a vSphere Client plug-in, vCenter Server snap-in, a command line interface (CLI), and REST API.

VCNS v5.5.0a is comprised of a suite of networking and security virtual appliances built for VMware vSphere integration. VMware vCenter Server provides centralized management of VMware's ESXi. VMware ESXi and vCenter Server 3.5, 4.0, 4.1, and 5.0 have been Common Criteria evaluated. ESXi is a user-installable or OEM-embedded virtualization layer that runs directly on industry standard x86-compatible hardware, providing an environment where multiple virtual machines can be hosted on one physical server.

A detailed description of the VCNS v5.5.0a architecture is found in Section 1 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for VCNS v5.5.0a is identified in Section 1.5 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
VMware Cryptographic Module	*Pending* [2]
VMware NSS Cryptographic Module	*Pending*
VMware Java JCE (Java Cryptographic Extension) Module	*Pending*
VMware Kernel Cryptographic Module	*Pending*

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in VCNS v5.5.0a:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	1660, 1661, 1662, 1663
Advanced Encryption Standard (AES)	FIPS 197	2771, 2772, 2773, 2774
Rivest Shamir Adleman (RSA)	FIPS 186-2	1447,1448, 1449, 1450
Secure Hash Algorithm (SHA-1)	FIPS 180-2	2328, 2329, 2330, 2331
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1733, 1734, 1735, 1736

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: VMware, Inc. vCloud Networking and Security 5.5.0a Security Target
Version: v1.8
Date: 19 February 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

VCNS v5.5.0a is:

a. *Common Criteria Part 2 extended*; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:

   FCS_HTTPS_EXT.1 – HTTPS;

   FCS_TLS_EXT.1 – TLS;

   DSM_SDC_EXT.1 - System data collection; and

   DSM_ANL_EXT.1 – Analysis.

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and

c. *Common Criteria EAL 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 – Flaw Reporting.

6 Security Policy

VCNS v5.5.0a implements a role-based access control policy to control user access to the system, as well as information flow control policies for Edge, Application and IPSEC functionality to control information entering the system; details of these security policies can be found in Section 7.1 of the ST.

In addition, VCNS v5.5.0a implements other policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TOE security functionality (TSF), trusted path/channel, and data security management. Further details on these security policies may be found in Section 7.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of VCNS v5.5.0a should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- Authorized administrators are non-hostile and follow all administrator guidance..
- Authorized administrators may access the TOE remotely from the internal and external networks.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Information cannot flow among the internal and external networks unless it passes through the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

8 Evaluated Configuration

The evaluated configuration for VCNS v5.5.0a comprises:

vShield App Hardware Requirements:
• Memory – 1 GB allocated, 1 GB reserved • Disk Space – 5 GB per vShield App per ESX host • vCPU – 2

vShield Edge Compact Hardware Requirements:
• Memory – 256 MB, Large and Quad Large: 1 GB, X-Large: 8GB • Disk Space – 300 MB, Large, Quad Large, and X-Large: 448 MB • vCPU – 1, Large: 2, Quad Large and X-Large: 4

vShield Endpoint and Data Security Hardware Requirements:
• Memory – 512 MB • Disk Space – 6GB per ESX host • vCPU – 1

vShield Manager Hardware Requirements:
• Memory – 8 GB allocated, 3 GB reserved • Disk Space – 60 GB • vCPU – 2

Required Supporting TOE Environment Software:
• VMware vCenter Server 5.1 • VMware ESXi 5.0 • VMware Tools

The publication entitled VMware vCNS v5.50a Guidance Supplement v0.6 describes the procedures necessary to install and operate VCNS v5.5.0a in its evaluated configuration.

9 Documentation

The VMware, Inc. documents provided to the consumer are as follows:

a. VMware vCNS v5.50a Guidance Supplement v0.6;

b. vShield Installation and Upgrade Guide vShield Manager 5.5, vShield Edge 5.5, vShield Endpoint 5.5;

c. vShield Administration Guide vShield Manager 5.5, vShield App 5.5, vShield Edge 5.5, vShield Endpoint 5.5;

d. vShield API Programming Guide vShield 5.5, vShield App 5.5, vShield Edge 5.5, vShield Endpoint 5.5; and

e. Command Line Interface Reference vShield Manager 5.1, vShield App 5.1, vShield Edge 5.1, vShield Endpoint 5.1.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of VCNS v5.5.0a, including the following areas:

Development: The evaluators analyzed the VCNS v5.5.0a functional specification and design documentation; they determined that the design completely and accurately describes the TTSF interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the VCNS v5.5.0a security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the VCNS v5.5.0a preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the VCNS v5.5.0a configuration management system and associated documentation was performed. The evaluators found that the VCNS v5.5.0a configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of VCNS v5.5.0a during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the VCNS v5.5.0a. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

11 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Security management through a firewall: The objective of this test goal was to verify the correct functionality of the TOEs management functions through a firewall;

c. PSK IPsec VPN functionality: The objective of this test goal is to demonstrate the correct functionality of the VPN using a PSK instead of a certificate;

d. VM separation: The objective of this test goal is to have the VM communicate using the vSphere plug-in instead of SSH; and

e. VM baseline: The objective of this test goal is to have the TOE scan a VM against an existing baseline.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Use of a traffic sniffer to view network traffic;

c. Filling the audit log in an attempt to lose recorded events;

d. Attempts to perform kernel, Tomcat, and SSH DoS attacks;

e. Using unauthenticated API commands in an attempt to gain access/information; and

f. Attempting to hijack the administrative session through manipulation of session Ids.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

11.4 Conduct of Testing

VCNS v5.5.0a was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CGI IT Security Evaluation & Test Facility . The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that VCNS v5.5.0a behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

While the CCEF did examine the possibility of a hostile entity interacting with the components and interfaces of the TOE, it is recommended that appropriate protections be placed upon the administrative interfaces of the TOE. This includes restricting access to these interfaces to only trusted individuals and regular reviews of the audit logs for the purposes of looking for suspicious activities.

The vCNS framework is extensible and can be leveraged by other products for the purposes of management (such as vCloud Director) or for implementing other functionality (such as Malware Protection). While this functionality was not reviewed in this evaluation the CCEF does note that the REST interface of the vShield Manager as well as the EPSEC libraries were examined for their secure operation. Additionally these modules were observed to have appropriate CAVP validation of their claimed cryptographic operation.

The CCEF notes that this is a product that assumes an appropriately knowledgeable administrator is upheld for configuration of the TOE, otherwise there could be potential for security misconfiguration. As such the CCEF notes that appropriate product knowledge should be given to the TOE administrator

The CCEF also notes that there is significant security functionality that is leveraged from the underlying layers such as vCenter and ESXi. As such the CCEF also recommends that the vCenter/ESXi administrator should have hands-on security expertise in order to maintain a secure posture of the infrastructure

The software lifecycle and patch schedule were examined as part of the flaw remediation activities and were found to positively impact the security posture of the TOE going forward while mitigating regression and interoperability issues through extensive testing. As such it is strongly recommended that the TOE administrator follow the VMware security advisories and apply any patches which would be relevant to their environment following the release of the TOE.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
API	Application Programming Interface
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CPL	Certified Products list
CM	Configuration Management
DoS	Denial of Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IPsec	Internet Protocol Security
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
PSK	Pre-shared key
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
SVM	Security Virtual Machine
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
VPN	Virtual Private Network

15 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. VMware, Inc. vCloud Networking and Security 5.5.0a Security Target, v1.8, 19 February 2014.

e. VMware vCloud Networking and Security 5.5.0a Common Criteria EAL4+ Evaluation ETR v0.6, February 26, 2014.