VMware, Inc.
3401 Hillview Ave
Palo Alto, CA 94304, USA
Tel: 877-486-9273
Email: info@vmware.com
http://www.vmware.com

VMware's Linux Cryptographic Module

Software Version: 2.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.5

vmware

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VMware's Linux Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware's Linux Cryptographic Module meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

This document also describes how to run the composite module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The VMware's Linux Cryptographic Module is also referred to in this document as “the module”.

1.2 Reference

This document deals only with operations and capabilities of the composite module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The VMware website (http://www.vmware.com) contains information on the full line of products from VMware.
- The CMVP website (https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search) contains options to get contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to VMware and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact VMware.

2 VMWARE'S LINUX CRYPTOGRAPHIC MODULE

2.1 NSX for vSphere

VMware, Inc. is a global leader in virtualization and cloud infrastructure, delivering customer-proven solutions that accelerate Information Technology (IT) by reducing complexity and enabling more flexible, agile service delivery. VMware enables enterprises to adopt a cloud model that addresses their unique business challenges. VMware's approach accelerates the transition to cloud computing while preserving existing investments and improving security and control.

VMware's Software Defined Data Center (SDDC) architecture is now extending virtualization technologies across the entire physical data center infrastructure. VMware NSX®, the network virtualization platform, is a key product in the SDDC architecture. With NSX, virtualization delivers for networking what it has already delivered for compute and storage. In much the same way that server virtualization programmatically creates, snapshots, deletes and restores software-based virtual machines (VMs), NSX network virtualization programmatically creates, snapshots, deletes, and restores software-based virtual networks. The result is a completely transformative approach to networking that not only enables data center managers to achieve orders of magnitude better agility and economics, but also allows for a vastly simplified operational model for the underlying physical network. With the ability to be deployed on any IP network, including both existing traditional networking models and next-generation fabric architectures from any vendor, NSX is a completely non-disruptive solution. In fact, with NSX, the physical network infrastructure you already have is all you need to deploy a software-defined data center.

2.1.1 NSX Components

This section describes the components of the NSX solution.

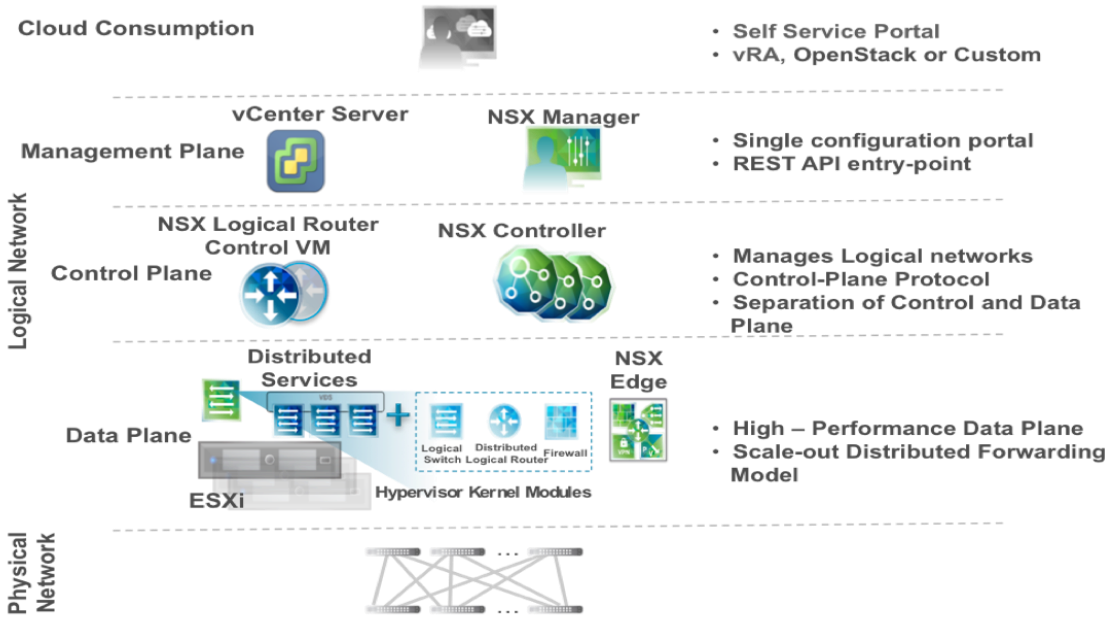

Figure 1 – NSX Components

Note that a cloud management platform (CMP) is not a component of NSX, but NSX provides integration into virtually any CMP via the REST API and out-of-the-box integration with VMware CMPs.

2.1.2 NSX Management Plane

The NSX management plane is built by the NSX Manager, the centralized network management component of NSX. It provides the single point of configuration and REST API entry-points.

The NSX Manager is installed as a virtual appliance on any ESX™ host in your vCenter Server environment. NSX Manager and vCenter have a one-to-one relationship. For every instance of NSX Manager, there is one vCenter Server. This is true even in a cross-vCenter NSX environment.

In a cross-vCenter NSX environment, there is both a primary NSX Manager and one or more secondary NSX Managers. The primary NSX Manager allows you to create and manage universal logical switches, universal logical (distributed) routers and universal firewall rules. Secondary NSX Managers are used to manage networking services that are local to that specific NSX Manager. There can be up to seven secondary NSX Managers associated with the primary NSX Manager in a cross-vCenter NSX environment.

2.1.3 NSX Control Plane

The NSX control plane runs in the NSX Controller cluster. NSX Controller is an advanced distributed state management system that provides control plane functions for NSX logical switching and routing functions. It is the central control point for all logical switches within a network and maintains information about all hosts, logical switches (VXLANs), and distributed logical routers.

The controller cluster is responsible for managing the distributed switching and routing modules in the hypervisors. The controller does not have any dataplane traffic passing through it.

2.1.4 NSX Edge

An integral part of the NSX solution is the ability to build an agile and trusted private cloud infrastructure as part of a virtual datacenter. It may be configured as an edge services gateway (ESG) or as a distributed logical router (DLR). In both configurations NSX Edge provides a wide range of services, including a highly available stateful inspection firewall, IPsec[1] site-to-site VPN[2], a server-load balancer, NAT[3], and network services such as static routing, DHCP[4] and DNS[5].

VPNs are essential for site-to-site communication over a shared network. NSX Edge protects the confidentiality of all data transmitted across virtual data center perimeters to remote sites using two VPN protocols: TLS[6] and the secure IPSec protocol. Both protocols provide the authentication and encryption of packets flowing between a remote site and the Edge-protected virtual data center for protected remote access.

2.1.5 VMware's Linux Cryptographic Module

Powering IPsec encryption and integrity in NSX Edge and NSX Controller is the VMware's Linux Cryptographic Module. The Tunnel mode of the Encapsulating Security Payload (ESP) protocol performed by an IPsec Service kernel stack, such as NETKEY, utilizes the VMware's Linux Cryptographic Module to

[1] IPsec – Internet Protocol Security
[2] VPN – Virtual Private Network
[3] NAT – Network Address Translation
[4] DHCP – Dynamic Host Configuration Protocol
[5] DNS – Domain Name System
[6] TLS – Transport Layer Security

encrypt, decrypt, and perform integrity checks on data entering and exiting the NSX Edge virtual appliance.

The VMware's Linux Cryptographic Module is a software cryptographic module located in the kernel space of the NSX Edge and NSX Controller virtual appliances. The module contains a set of cryptographic functions available to an IPSec kernel stack via a well-defined Application Programming Interface (API). These functions facilitate the secure transfer of information between:

- VMware's NSX Edge Security Appliance and a remote peer attempting to connect to an Edge-protected network.
- Cluster intercommunication between NSX Controllers

The module includes implementations of the following FIPS-Approved security functions:

- Encryption and decryption using AES[7]
- Hashing functions using SHA[9] & HMAC[10] SHA

The VMware's Linux Cryptographic Module is validated at the FIPS 140-2 Section levels shown in Table 1:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A[11]
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[12]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The VMware's Linux Cryptographic Module is a software cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The module was tested and found to be FIPS 140-2 compliant on a Dell PowerEdge T620 Server running an Intel Xeon E5 processor, executing VMware vSphere Hypervisor (ESXi) 6.0 using the supported OS list below. The composite module is composed of 2 components:

- VMware's Linux Cryptographic Module – Cryptographic algorithm implementations located in the kernel-level of the OS versions listed below. These implementations are leveraged by the IPsec Service implementation located in the user-space in order to perform an IPsec tunnel.
    - NSX Edge 6.3.0 OS (AKA NSX Edge 3.14 OS)

[7] AES – Advanced Encryption Standard
[9] SHA – Secure Hash Algorithm
[10] HMAC – (Keyed) Hash Message Authentication Code
[11] N/A – Not Applicable
[12] EMI/EMC – Electromagnetic Interference/Electromagnetic Compatibility

  - NSX Controller 6.3.0 OS (AKA NSX Controller 12.04 OS)
  - NSX OS 4.4 (AKA BLUX 4.4)
  - PhotonOS 1.0
  - PhotonOS 2.0
- OpenSSL command line utility – Integrity mechanism located in the User space of the supported OS versions. This mechanism coordinates the integrity check on itself as well as the entire supported OS kernels, which includes the VMware's Linux Cryptographic Module. The mechanism leverages the HMAC SHA-512 algorithm implemented in the FIPS validated VMware OpenSSL FIPS Object Module.

The following component (a bound module) needs to be installed for the VMware's Linux Cryptographic Module to operate:

- VMware OpenSSL FIPS Object Module (FIPS Certificate #2839) – The VMware OpenSSL FIPS Object Module is a bound FIPS validated cryptographic module located in the User space of the supported OS versions. The OpenSSL command line utility leverages the HMAC SHA-512 implementation of the VMware OpenSSL FIPS Object Module in order to perform an integrity check on the entire supported OS kernels.

Further, VMware, Inc. affirms that the VMware's Linux Cryptographic Module runs in its configured, Approved mode of operation on the following binary compatible platforms executing VMware vSphere Hypervisor (ESXi) 6.0, 6.5, and 6.7:

- A general-purpose computing platform with an AMD Opteron x86 Processor executing VMware NSX for supported OS versions.
- A general-purpose computing platform with an Intel Core i3, Core i5, Core i7, or Xeon Processor executing VMware NSX for the supported OS versions.
- A cloud computing environment composed of the above general-purpose platform executing VMware NSX or a VMware cloud solution that is executing VMware NSX.

In addition to its full AES software implementations, the VMware's Linux Cryptographic Module is capable of leveraging the AES-NI[13] instruction set of supported Intel processors in order to accelerate AES calculations.

Because the VMware's Linux Cryptographic Module is defined as a software cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary.

2.2.1 Physical Cryptographic Boundary

As a software module, the module must rely on the physical characteristics of the host system. The physical boundary of the cryptographic module is defined by the hard enclosure around the host system on which it runs. The module supports the physical interfaces of the Dell PowerEdge T620 Server. These interfaces include the integrated circuits of the system board, processor, RAM, hard disk, device case, power supply, and fans. See Figure 2 below for a block diagram of the Dell PowerEdge T620 Server.

[13] AES-NI – Advanced Encryption Standard-New Instructions

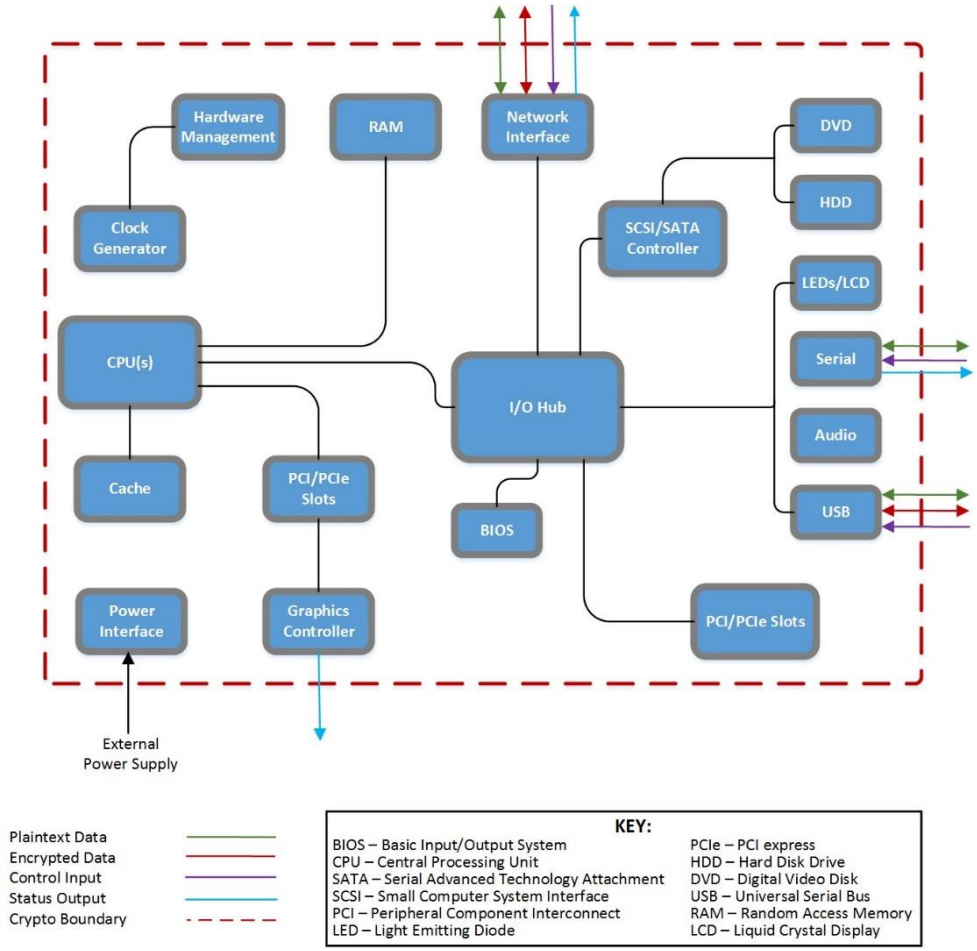

Figure 2 – Hardware Block Diagram

2.2.2 Logical Cryptographic Boundary

Figure 3 depicts the logical cryptographic boundary for the composite module which surrounds the VMware's Linux Cryptographic Module and the OpenSSL command line utility. The FIPS 140-2 validated VMware OpenSSL Cryptographic Module is a bound module that provides its HMAC SHA-512 algorithm implementation to perform the module's integrity test.

The colored arrows indicate the logical information flows into and out of the module. The module is shown exchanging data with the Linux native NETKEY Stack which is also located in the kernel space of the operating system. The IPSec Service in the user space of the operating system makes system calls to the Linux native NETKEY Stack.

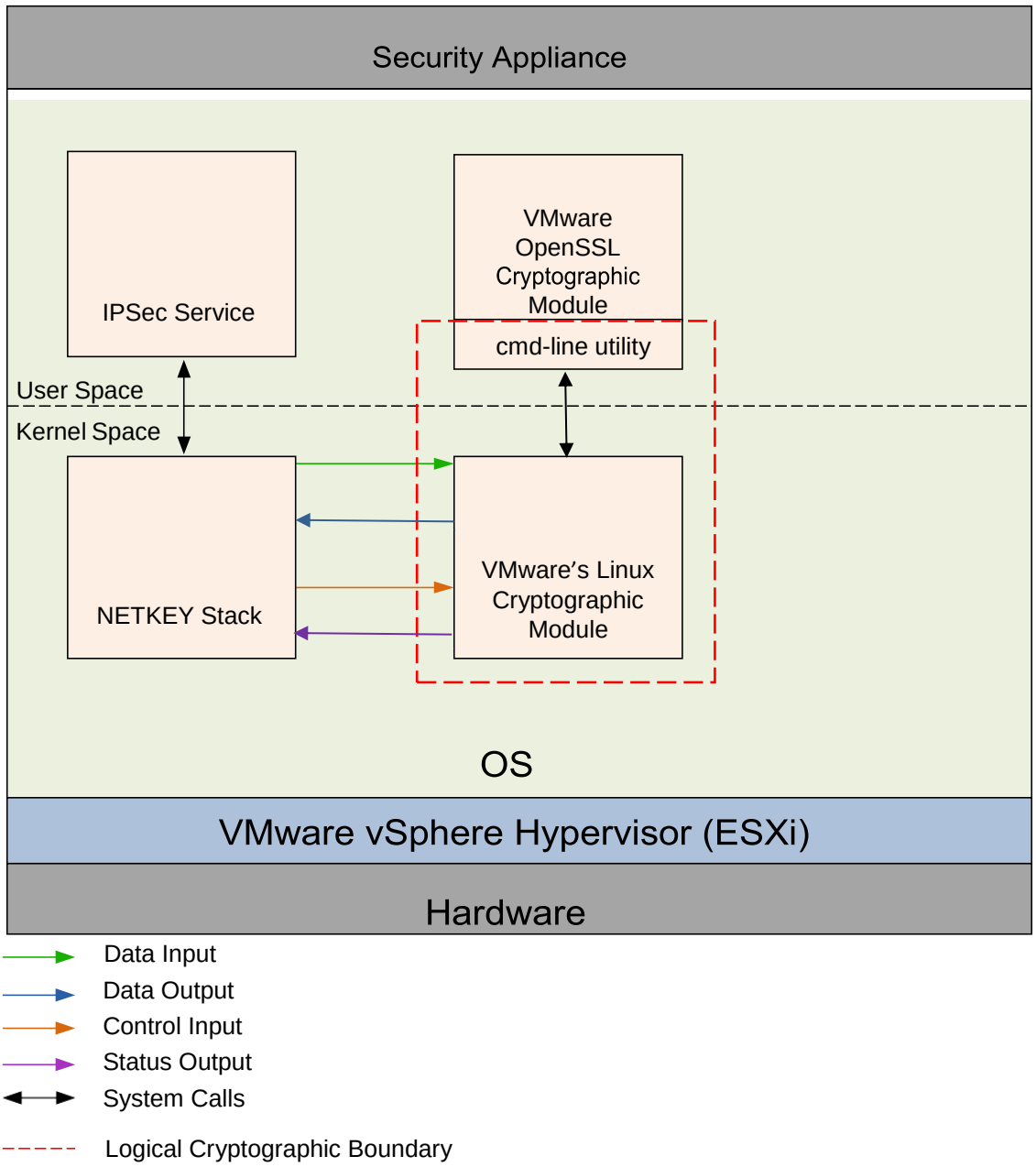

Figure 3 – Module's Logical Cryptographic Boundary

The module implements the FIPS-Approved algorithms listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	With AES-Ni	In Software
AES in ECB and CBC mode (encryption/decryption) with 128, 192, and 256-bit keys	4133	4133
SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512		3402
HMAC with SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512		2705

When used for the integrity check of the module, the VMware OpenSSL Cryptographic Module provides the following Approved functions:

- HMAC with SHA-512 (Cert #2710)

The key establishment methodology for the algorithms used in this module is outside of the composite module's cryptographic boundary.

The composite module employs non-compliant algorithms and associated services, which are not allowed for use in a FIPS-Approved mode of operation. Their use will result in the module operating in a non-Approved mode. Please refer to Table 3 below for the list of non-Approved algorithms and associated services.

Table 3 – Non-Approved Algorithms and Services

Service	CSP and Type of Access
Encryption (Non-Compliant)	AES XTS Key (Non-Compliant) Triple-DES (Non-Compliant) DES
Decryption (Non-Compliant)	AES XTS Key (Non-Compliant) Triple-DES (Non-Compliant) DES

2.3 Module Interfaces

The module's logical interfaces exist at a low level in the software as an API. Both the API and physical interfaces can be categorized into the following interfaces defined by FIPS 140-2:

- Data input
- Data output
- Control input
- Status output
- Power input

As a software module, the module's manual controls, physical indicators, and physical and electrical characteristics are those of the host platform. A mapping of the FIPS 140-2 logical interfaces, the physical interfaces, and the module interfaces can be found in Table 4 below.

Table 4 – FIPS 140-2 Logical Interface Mapping

FIPS Interface	Physical Interface	Level
Data Input	Network port, Serial port, USB port, SCSI/SATA Controller	The function calls that accept input data for processing through their arguments.
Data Output	Network port, Serial port, USB port, SCSI/SATA Controller	The function calls that return by means of their return codes or argument generated or processed data back to the caller.
Control Input	Network port, Serial port, USB port, Power button	The function calls that are used to initialize and control the operation of the module.
Status Output	Network port, Serial port, USB port, Graphics controller	Return values for function calls; Module generated error messages.
Power Input	AC Power socket	Not applicable.

2.4 Roles and Services

There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Cryptographic Officer (CO) role and a User role. Roles are assumed implicitly through the execution of either a CO or User service. The module does not support an authentication mechanism. Each role and their corresponding services are detailed in the sections below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 5 below indicates the types of access required using the following notation:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an FIPS-Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto Officer and User Roles

The CO and User roles share many services, including encryption, decryption, and random number generation services. The CO performs installation and initialization, show status, self-tests on demand, and key zeroization services. Table 5 below describes the CO and User services and Table 3 describes the Non-Approved CO & User services.

Table 5 – Crypto Officer and User Services

Role	Service	Description	CSP and Type of Access
CO, User	Encryption	Encrypt plaintext using supplied key and algorithm specification	AES Key – RX
CO, User	Decryption	Decrypt ciphertext using supplied key and algorithm specification	AES Key – RX
CO, User	Hash generation	Compute and return a message digest using SHA algorithm	None
CO, User	Message Authentication Code generation	Compute and return a hashed message authentication code	HMAC Key - RX
CO	Installation and initialization of the module	Installation and initialization of the module following the Secure Operation section of the Security Policy	None

CO	Show status	Returns the current mode of operation of the module	None
CO	Run Self-tests on demand	Runs Self-tests on demand during module operation	None
CO	Key zeroization	Zeroizes keys	None

2.5 Physical Security

The VMware's Linux Cryptographic Module is a software module, which FIPS defines as a multiple-chip standalone cryptographic module. As such, it does not include physical security mechanisms. Thus, the FIPS 140-2 requirements for physical security are not applicable.

2.6 Operational Environment

The module was tested and found to be compliant with FIPS 140-2 requirements on a Dell PowerEdge T620 Server with an Intel Xeon E5-2440 processor running VMware vSphere Hypervisor (ESXi) 6.0 and the supported OS versions mentioned in Section 2.2. All cryptographic keys and CSPs are under the control of the OS, which protects its CSPs against unauthorized disclosure, modification, and substitution. The module only allows access to CSPs through its well-defined API.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6.

Table 6 – List of Cryptographic Keys, Key Components, and CSPs

Key	Key Type	Generation/ Input	Output	Storage	Zeroization	Use
AES key	128, 192, 256-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	In RAM	Reboot OS; Cycle host power	Encryption, Decryption
HMAC key	112-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	In RAM	Reboot OS; Cycle host power	Message Authentication

2.8 Self-Tests

Cryptographic self-tests are performed by the module when the module is powered on. The following sections list the self-tests performed by the module, their expected error status, and any error resolutions.

2.8.1 Power-Up Self-Tests

Power-up self-tests are automatically performed by the module at module initialization or when the module powers on. The list of power-up self-tests that follows may also be run on-demand when the CO reboots the Operating System. The module will perform the listed power-up self-tests to successful completion. During the execution of self-tests, data output from the module is inhibited.

If any of the self-tests fail, the module will return an error and will remain in an error state. After entering the error state, all subsequent calls to the module requiring data output will be rejected, ensuring that data output from the module is inhibited. In order to resolve a self-test error, the module must be restarted by rebooting the OS. If the error persists, the module must be reinstalled.

The VMware's Linux Cryptographic Module performs the following Power-up Self-tests:

- Software integrity check (HMAC SHA-512 Integrity Test) - The software integrity test is performed by the OpenSSL command line utility, which coordinates the integrity check of the entire supported OS kernels (Section 2.2).
    1. The utility loads the VMware OpenSSL Cryptographic Module. The VMware OpenSSL Cryptographic Module performs its own integrity check using the HMAC SHA-256 algorithm.
    2. The utility performs the integrity check of its own file using the HMAC SHA-512 implementation provided by the VMware OpenSSL Cryptographic Module.
    3. The utility performs the integrity check on the rest of the VMware's Linux Cryptographic Module using the HMAC SHA-512 implementation provided by the VMware OpenSSL Cryptographic Module.
- Known Answer Tests (KATs)
    - AES Encryption KAT
    - AES Decryption KAT
    - SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 KAT
    - HMAC SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 KAT

2.8.2 Conditional Self-Tests

The module does not implement any algorithm or function that requires a conditional self-test

2.9 Mitigation of Other Attacks

This section is not applicable. The module was not designed to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 SECURE OPERATION

The VMware's Linux Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Crypto Officer Guidance

Installation and operation of the VMware's Linux Cryptographic Module requires the proper installation of the NSX Edge and NSX Controller virtual appliances. The sections below provide a brief summary of the installation procedures for NSX Edge. For a more comprehensive instruction set, please refer to the *NSX Installation Guide* provided by VMware.

All guides mentioned within these instructions are available for download at http://www.vmware.com. These instructions assume that the CO is familiar with VMware vSphere Hypervisor (ESXi) 6.0 and VMware NSX for vSphere 6.3.0 products.

3.1.1 Initial Setup

Prior to the secure installation of the NSX for vSphere, the CO shall prepare the virtual environment required to securely operate the virtual appliance. This includes installing VMware vSphere Hypervisor (ESXi) 6.0 (see *vSphere Installation and Setup*). Included in this installation are the VMware vSphere Hypervisor (ESXi) 6.0, vSphere 6.0 vSphere Client, and the vSphere 6.0 vCenter Server, all of which are prerequisites to installing the NSX for vSphere.

After installing the VMware vSphere 6.0 virtual environment, the CO shall log into the vCenter Server using the vSphere Client and follow the instructions provided in Chapter 3 of *NSX Installation Guide* to securely install and configure NSX for vSphere Manager Virtual Appliance; the management component needed to install NSX Edge.

3.1.2 Secure Installation

In order to install the NSX Edge version of the VMware's Linux Cryptographic Module, the CO shall follow the installation instructions provided in Chapter 18 of *NSX Installation Guide* in order to securely install and configure the NSX Edge Virtual Appliance. A brief summary of the installation steps is provided:

- Log into the vCenter Server using vSphere Client
- Determine which ESXi host the virtual appliance will be installed on
- Access the "Add Edge" dialog
- Complete the rest of the Edge configurations
- Create and deploy the Edge Appliance
- Confirm the settings and install

In order to install the NSX Controller version of the VMware's Linux Cryptographic Module, the CO shall follow the installation instructions provided in Chapter 8 of *NSX Installation Guide* in order to securely install and configure the NSX Controller Virtual Appliance. A brief summary of the installation steps is provided:

- Log into the vCenter Server using vSphere Client
- Determine the setting for the Controller virtual appliance
- Access the "Add Controller" dialog
- Configure an IP Pool for the Controller cluster
- Complete the rest of the Controller configurations

- Confirm the settings and install
- After the first Controller is deployed, add two more Controllers (NSX requires 3 controllers)

Using the vSphere Client, the CO can determine that the virtual appliances are operational. Troubleshooting is available in Section 23 of the *NSX Installation Guide*.

3.1.3 VMware's Linux Cryptographic Module Secure Operation

Following the successful installation of the NSX Edge and NSX Controller virtual appliances, the CO shall power on the virtual appliance. The module is loaded at the time of the system boot. The CO shall follow the guidelines in Chapter 9 of the *NSX Administration Guide, or follow the instructions mentioned below* in order to securely configure and operate the VMware's Linux Cryptographic Module.

For NSX OS, Edge, and Controller kernels:

Edit the file /boot/grub/grub.cfg, and change "set default=0" to "set default=1". 0 is non FIPS mode, 1 is FIPS mode.

For Photon kernels:

Edit the file /boot/photon.cfg, add "fips=1" to the end of the "photon_cmdline" assignment.

The module will continue to operate in the FIPS mode of operation unless it is disabled by changing the configuration. The OpenSSL command line utility leverages the FIPS validated VMware OpenSSL Cryptographic Module one time during the boot up of the module until it has completed the module's integrity test successfully. Both the OpenSSL command line utility and VMware OpenSSL Cryptographic Module are not utilized again (with respect to this module) until another integrity check is required. To verify that the VMware's Linux Cryptographic Module is operating in the FIPS Approved mode: the CO can verify the file /proc/sys/crypto/fips_enabled exists, and contains "1".

3.2 User Guidance

The VMware's Linux Cryptographic Module is designed for use by the VMware NSX Edge and VMware NSX Controller appliances. The User shall adhere to the guidelines of this Security Policy. The User does not have any ability to install or configure the module. Operators in the User role are able to use the services available to the User role listed in Table 5. The User is responsible for reporting to the CO if any irregular activity is noticed. The FIPS validated VMware OpenSSL Cryptographic Module, although used, is only considered to support the integrity verification and is not intended for general-purpose use with respect to this module.

4 ACRONYMS

Table 7 provides definitions for the acronyms used in this document.

Table 7 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CPU	Central Processing Unit
CSE	Communication Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DVD	Digital Video Disc
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HDD	Hard Disk Drive
HMAC	(Keyed) Hash Message Authenticating Code
INT	A validated Cryptographic Module which lies internal or inside of the boundary in regard to the reference diagram CM software physical boundary
IPsec	Internet Protocol Security
IT	Information Technology

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com