VMware, Inc.

VMware NSS Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS SECURITY LEVEL 1
DOCUMENT VERSION: 1.1

vmware®

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the VMware NSS Cryptographic Module from VMware, Inc. This Security Policy describes how the VMware NSS 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 http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This Security Policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The VMware NSS Cryptographic Module is referred to in this document as the VNCM, the crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the 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 (www.vmware.com) contains information on the full line of products from VMware.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains 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

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to VMware. 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 NSS Cryptographic Module

2.1 vCloud Networking and Security

VMware, Inc. is a global leader in virtualization and cloud infrastructure, delivering customer-proven solutions that accelerate 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.

One of the many virtualization products that VMware delivers to the market is vCloud Networking and Security (vCNS). vCNS provides software defined networking and security built into the virtual infrastructure. Just as VMware vSphere® abstracts processing capacity from server hardware to create virtual pools of resources that can be consumed as a service, vCNS abstracts networking and security into a generalized pool of capacity and separates the consumption of these services from the underlying physical infrastructure. vCNS is a networking and security solution which provides virtual firewalls, virtual private networks (VPNs), and load balancing to virtual datacenters and private cloud deployments. Three key virtual security appliances are part of the vCNS solution:

- vShield Manager - A central management and reporting tool for vCNS components
- vShield Edge - A networking and security gateway for protecting virtual data centers
- vShield App - A virtual firewall to protect critical applications on virtual machines

Additional components that make up the vCNS suite include vShield Endpoint and vShield Data Security.

vCNS is typically used in the following scenarios:

- Secure Virtualization of Business-Critical Applications
- Build an Agile and Trusted Private Cloud Infrastructure
- Secure Virtual Desktop Deployments

Figure 1 illustrates an idealized deployment scenario for the vCloud Networking and Security solution.

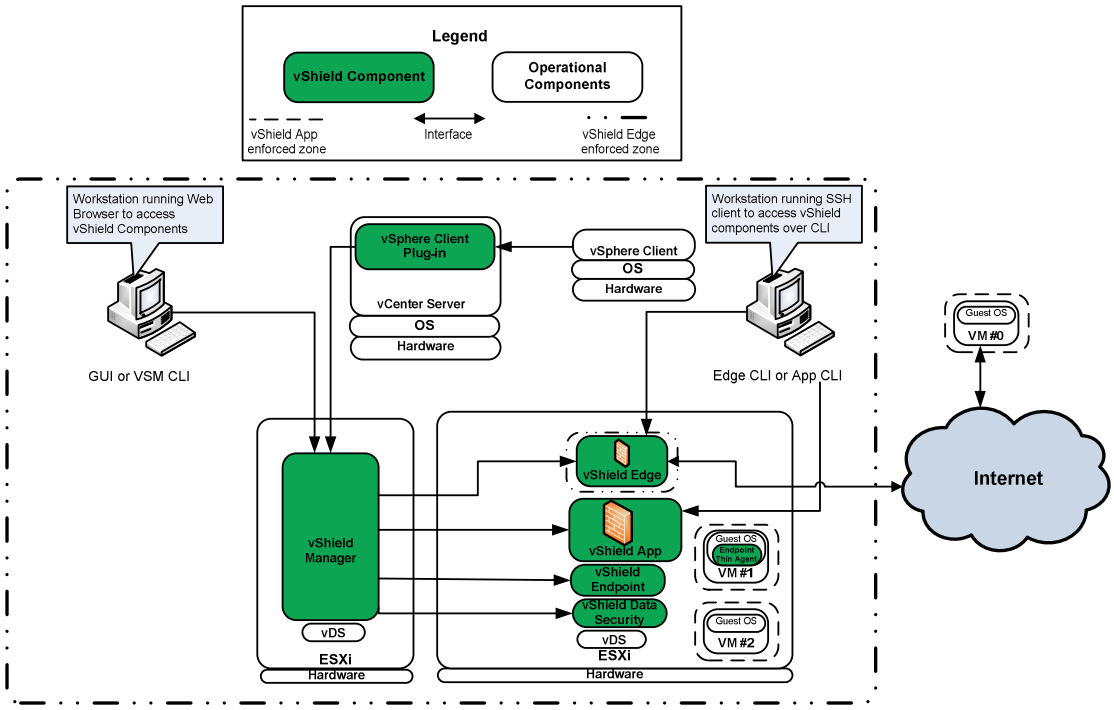

Figure 1 – vCloud Networking and Security Sample Deployment

2.1.1 VMware vShield Edge

An integral part of the vCNS solution is the ability to build an agile and trusted private cloud infrastructure as part of a virtual datacenter. The Edge Gateway appliance establishes a perimeter gateway for network traffic to enter and leave a virtual datacenter. It provides a wide range of services, including a highly available stateful inspection firewall, an IPsec[1] site-to-site VPN[2], a server-load balancer, network-address translation and network services including static routing, DHCP[3] and domain name system (DNS). Common deployments of vShield Edge include placing it in a DMZ[4], on a VPN Extranet, or in multitenant Cloud environments where the vShield Edge provides perimeter security for Virtual Datacenters (VDCs).

Virtual Private Networks are essential for site-to-site communication over a shared network. vShield Edge protects the confidentiality of all data transmitted across virtual data center perimeters to remote sites using the secure IPsec[5] protocol. IPsec provides the authentication and encryption of packets flowing between a remote site and the Edge-protected virtual data center for protected remote access. vShield Edge utilizes IPsec to provide secure access to the Edge-protected network.

2.1.2 IPSec Service

Edge includes an IPSec Service to provide a complete implementation of IPsec and Internet Key Exchange (IKE)[6]. The service is capable of interoperating with other IPsec and IKE enabled systems that have previously been deployed on external networks. It is installed as part of the standard vShield Edge deployment.

[1] IPsec – Internet Protocol Security
[2] VPN – Virtual Private Network
[3] DHCP – Dynamic Host Configuration Protocol
[4] DMZ – Demilitarized Zone
[5] IPsec – Internet Protocol Security
[6] This protocol has not been reviewed or tested by the CAVP and CMVP

The vShield Edge uses the IPsec Service to provide secure VPN connections from a remote site to the vShield Edge-protected network. The service provides encryption and authentication of packets communicated to the vShield Edge Virtual Appliance. In order to provide FIPS-Approved encryption, decryption, and authentication, the IPsec Service utilizes the cryptography provided by the VMware NSS Cryptographic Module.

2.1.3 VMware NSS Cryptographic Module

The VMware NSS Cryptographic Module (VNCM) is a software cryptographic module containing a set of cryptographic functions available to the IPsec Service via a well-defined Application Programming Interface (API). These functions facilitate the secure transfer of information between VMware's vShield Edge Virtual Security Appliance and a remote peer attempting to connect to an Edge-protected network. The VNCM is a shared cryptographic library which provides the FIPS-Approved algorithms necessary for VPN connections to the vShield Edge using the IPsec Service. The VNCM includes implementations of the following FIPS-Approved security functions:

- Hardware-accelerated Advanced Encryption Standard (AES) algorithm
- Symmetric key functions using Triple DES[7]
- Hashing functions using SHA[8]
- Asymmetric key functions using RSA[9]
- Random number generation using NIST SP[10] 800-90A Hash-based DRBG[11]

Figure 2 provides an idealized deployment scenario for the vShield Edge Virtual Security Appliance. The IPsec Service and the VMware NSS Cryptographic Module lie within the vShield Edge Virtual Appliance boundary (shown as the transparent, teal box). The IPsec Service provides secure VPN access to a vShield Edge-protected network (Secure/Isolated Network), to remote workstations on an unprotected internal network, or to remote machines on an external network (Unprotected Network and External Network). Multiple subnets can be configured to connect to the secure network behind the vShield Edge through IPsec tunnels. The VNCM provides the IPsec FIPS-Approved cryptographic services used by the IPsec Service.

[7] DES – Data Encryption Standard
[8] SHA – Secure Hash Algorithm
[9] RSA – Rivest, Shamir, Adleman
[10] SP – Special Publication
[11] DRBG – Deterministic Random Bit Generator

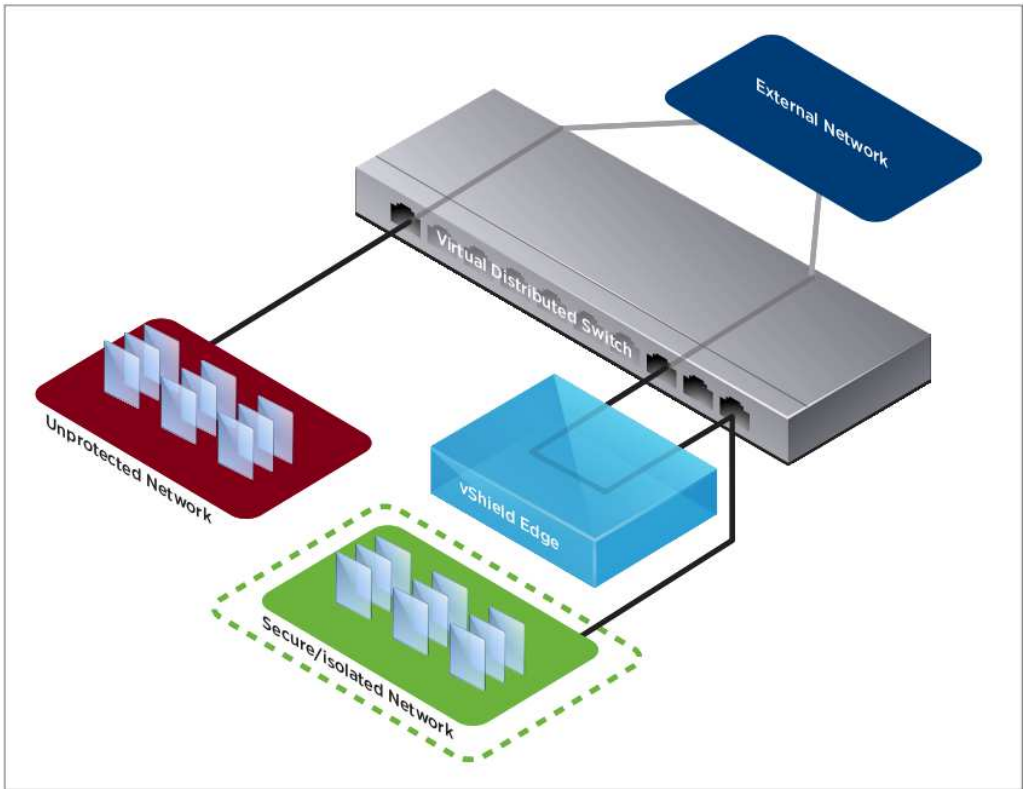

Figure 2 – vShield Edge Deployment Diagram

The VMware NSS Cryptographic Module is validated at 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
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

[12] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.2 Module Specification

The VMware NSS Cryptographic Module is a software cryptographic module with a multi-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 HP ProLiant DL380e Gen8 Server running an Intel Xeon E5-2430 processor executing VMware vCloud Networking and Security 5.5.0a Edge OS and VMware vSphere Hypervisor (ESXi) 5.5.

VMware, Inc. affirms that the VMware NSS Cryptographic Module runs in its configured, Approved mode of operation on the following binarily compatible platforms executing VMware vSphere Hypervisor (ESXi) 5.5:

- A general purpose computing platform with an AMD Opteron x86 Processor executing VMware vCloud Networking and Security 5.5.0a Edge OS.
- A general purpose computing platform with an Intel Core i3, Core i5, Core i7, and Xeon x86 Processor executing VMware vCloud Networking and Security 5.5.0a Edge OS.

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

Because the VMware NSS Cryptographic Module is defined as a software cryptographic module, it possesses both a physical cryptographic boundary and a logical cryptographic boundary. The physical and logical boundaries are outlined in Section 2.2.1 and 2.2.2, respectively.

2.2.1 Physical Cryptographic Boundary

As a software cryptographic 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 HP ProLiant. These interfaces include the integrated circuits of the system board, processor, network adapters, RAM[14], hard disk, device case, power supply, and fans. See Figure 3 for a block diagram of the HP ProLiant.

[13] AES-NI – Advanced Encryption Standard-New Instructions
[14] RAM – Random Access Memory

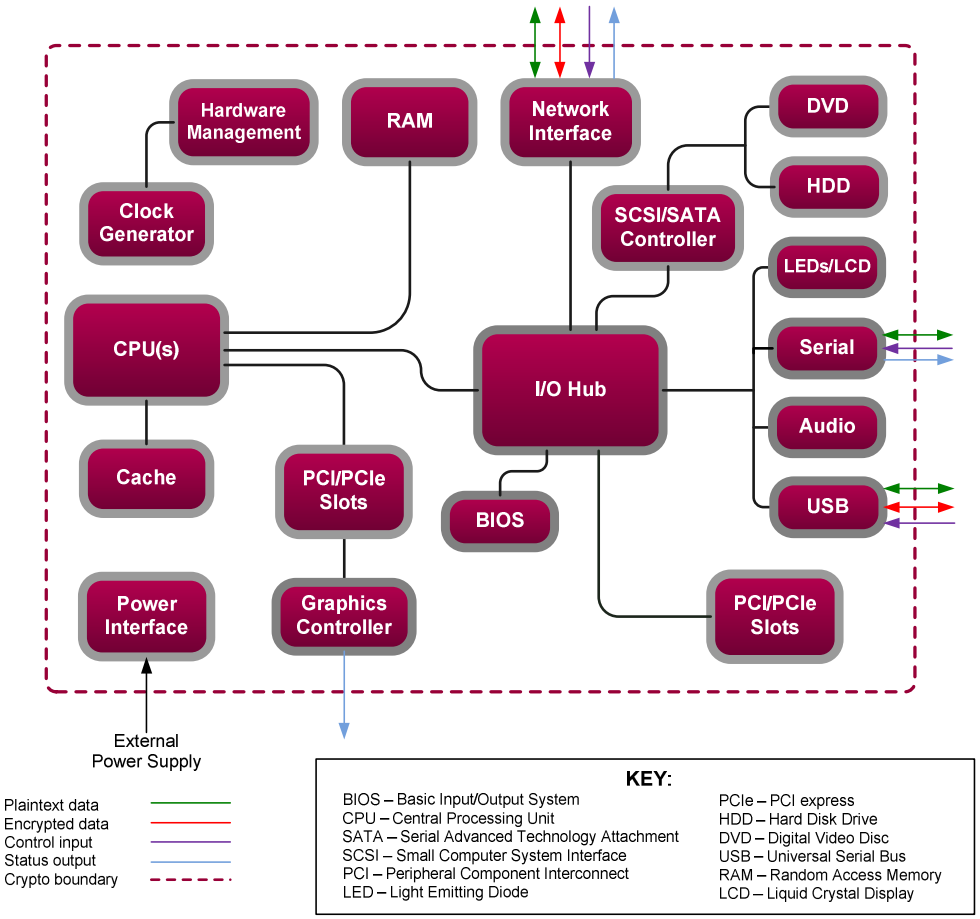

Figure 3 – HP ProLiant Server Block Diagram

2.2.2 Logical Cryptographic Boundary

Figure 4 shows a logical block diagram of the module executing in memory and its interactions with surrounding software components, as well as the module's logical cryptographic boundary. The files and binaries that make up the software component of the cryptographic module are shown as "VMware NSS Cryptographic Module" in the diagram below. The module's services are designed to be called by applications such as the IPsec Service. The module's logical boundary is a contiguous perimeter that surrounds all memory-mapped functionality provided by the module when loaded and stored in the host platform's memory.

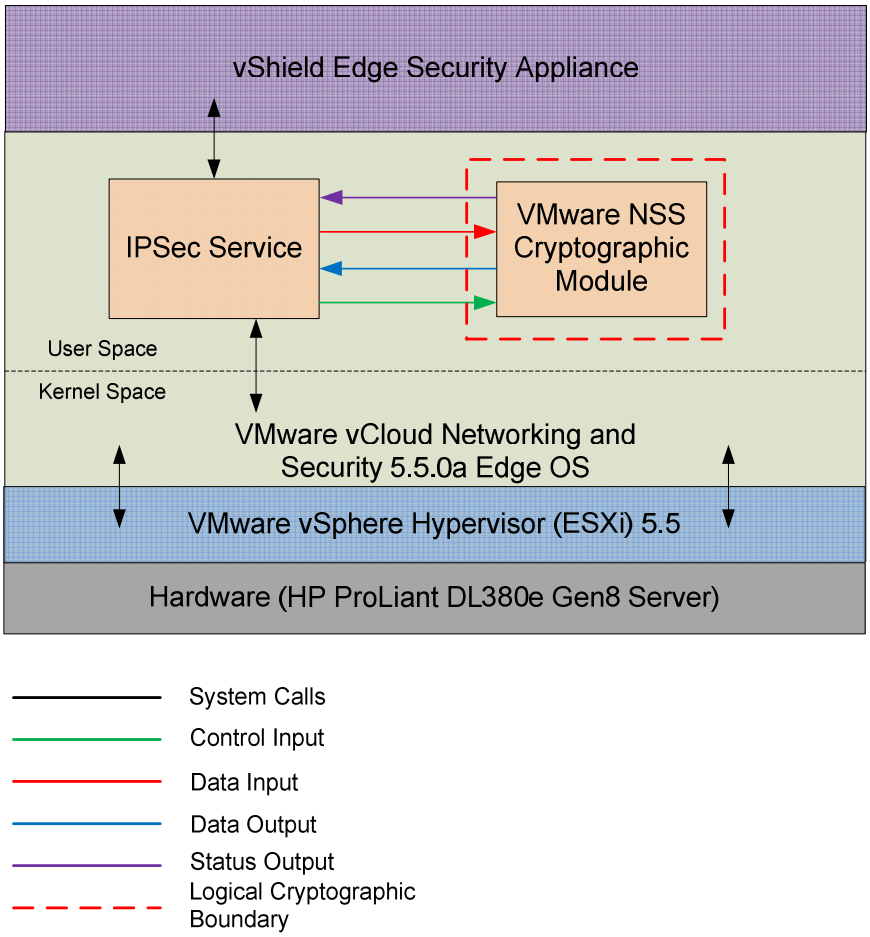

Figure 4 – VMware NSS Cryptographic Module Logical Cryptographic Boundary

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 has no physical characteristics. Thus, 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 2 below.

Table 2 – FIPS 140-2 Logical Interface Mappings

FIPS Interface	Physical Interface	Module Interface (API)
Data Input	Network port, Serial port, SCSI/SATA Controller, USB port	The function calls that accept input data for processing through their arguments.
Data Output	Network port, Serial port, SCSI/SATA Controller, USB port	The function calls that return by means of their return codes or arguments 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

The module does not support an authentication mechanism. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer (CO) role and a User role. Roles are assumed implicitly through the execution of either a CO or User service. 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 3 and Table 4 below indicate 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 Approved or Allowed security function or authentication mechanism.

2.4.1 Crypto Officer Role

To assume the CO role, an operator of the module will perform one of the services listed in Table 3. The CO has the ability configure the module, run self-tests on demand, show status, and zeroize all keying material.

Table 3 – Crypto Officer Services

Service	Description	CSP and Type of Access
Initialize FIPS mode	Performs integrity check and power-up self-tests. Sets the FIPS-Approved mode flag to on.	None
Run self-tests on demand	Performs power-up self-tests	None
Show status	Returns the current mode of the module	None
Zeroize key	Zeroizes and de-allocates memory containing sensitive data	All keys – W

2.4.2 User Role

To assume the User role, an operator of the module will perform one of the services listed in Table 4. The User has the ability to generate random numbers, symmetric and asymmetric keys, and digital signatures.

Table 4 – User Services

Service	Description	CSP and Type of Access
Generate random number	Returns the specified number of random bits to calling application	DRBG Seed – RWX DRBG C Value – RW DRBG V Value – RW
Generate message digest (SHS[15])	Compute and return a message digest using SHS algorithms	None
Generate Keyed Digest	Computer and return a keyed message digest	HMAC Key – WRX
Generate Symmetric Key	Compute and return a symmetric key for encryption and decryption	AES Key – W Triple-DES Key – W
Symmetric encryption	Encrypt plaintext using supplied key and algorithm specification	AES key – RX Triple-DES key – RX
Symmetric decryption	Decrypt ciphertext using supplied key and algorithm specification	AES key – RX Triple-DES key – RX
RSA key wrapping	Wrap keys using RSA public key (used for key transport)	RSA public key – RX
RSA key unwrapping	Unwrap keys using RSA private key (used for key transport)	RSA private key – RX
DH[16] key agreement	Perform key agreement using Diffie-Hellman algorithm	DH public and private keys – WX
Generate Asymmetric Keys	Generate a public and private key pair	DSA public key – W DSA private key – W
Signature Generation	Generate a signature for the supplied message using the specified key and algorithm	RSA private key – RX DSA private key – RX

[15] SHS – Secure Hash Standard
[16] DH – Diffie-Hellman

Service	Description	CSP and Type of Access
Signature Verification	Verify the signature on the supplied message using the specified key and algorithm	RSA public key – RX DSA public key – RX

2.5 Physical Security

The VMware NSS Cryptographic Module is a software module, which FIPS defines as a multi-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 HP ProLiant DL380e Gen8 Server with an Intel Xeon E5-2430 processor[17] running VMware vSphere Hypervisor (ESXi) 5.5 and VMware vCloud Networking and Security 5.5.0a Edge OS. 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 following sections highlight the module's cryptographic keys and critical security parameters.

2.7.1 Approved Cryptographic Algorithms

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES in ECB[18], CBC[19] modes with 128- , 192-, and 256- bit keys	2700
AES (Hardware-accelerated) in ECB, CBC modes with 128- , 192-, and 256- bit keys	2700
Tripe-DES in ECB, CBC modes; KO[22] 1	1619
SHA-1, SHA-256, SHA-384, and SHA-512	2267
HMAC with SHA-1, SHA-256, SHA-384, SHA-512	1681
RSA (PKCS[23] #1 v1.5) Signature Generation 2048- and 3072-bits	1398
RSA (PKCS #1 v1.5) Signature Verification 1024-, 1536-, 2048-, 3072-, and 4096-bits	1398
DSA 1024-bit Signature Verification	821
DSA PQG 1024-bit Signature Verification	821

[17] The module was tested on the same processor with AES-NI support turned on and tested again with AES-NI support turned off
[18] ECB – Electronic Code Book
[19] CBC – Cipher Block Chaining
[22] KO – Key Option
[23] PKCS – Public Key Cryptography Standard

Algorithm	Certificate Number
SP 800-90A Hash DRBG	443

The module employs the following key establishment methodology, which is allowed for use in a FIPS-Approved mode of operation:

- RSA Key wrapping; key establishment methodology provides 112 to 150[24] bits of encryption strength; non-compliant less than 112 bits of encryption strength
- Diffie-Hellman Key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength
- EC Diffie-Hellman Key agreement; key establishment methodology provides between 112 and 256 bits of encryption strength; non-compliant less than 112 bits of encryption strength

Caveats:

- Additional information concerning SHA-1, Diffie-Hellman key agreement/key establishment, RSA 1024-bit signature generation, RSA key transport, DSA key generation, DSA signature generation, and specific guidance on transitions to the use of stronger cryptographic keys and more robust algorithms is contained in NIST Special Publication 800-131A.

- The module generates cryptographic keys whose strengths are modified by available entropy

2.7.2 Non-Approved Cryptographic Algorithms and Services

The module employs non-Approved cryptographic algorithms and services, which are accessible by the operator of the module. The use of these algorithms and services leads the module to operate in the non-Approved mode of operation. Their use, while operating in the FIPS-Approved mode, is strictly prohibited. Table 6 lists the non-Approved algorithms services provided by the module.

Table 6 – VMware NSS Cryptographic Module Non-Approved Algorithms and Services

Algorithm	Non-Compliant Service
RC2[25]	Encryption; Decryption
RC4	Encryption; Decryption
DES	Encryption; Decryption
SEED	Encryption; Decryption
CAMELLIA	Encryption; Decryption
Triple-DES with KO2	Encryption; Decryption
MD2[26]/MD5	Hashing
ECDSA[27] (non-compliant)	Digital Signature Generation/Verification
Diffie-Hellman (non-compliant)	Key Agreement; Key Establishment (components < 112 bits in strength)

[24] Derived per equation 1 of IG 7.5
[25] RC – Rivest Cipher
[26] MD – Message Digest
[27] ECDSA – Elliptic Curve DSA

Algorithm	Non-Compliant Service
ECDH[28] (non-compliant)	Key Agreement; Key Establishment (components < 112 bits in strength)
HKDF[29]	Symmetric Key Derivation
J-PAKE[30]	Symmetric Key Exchange
DSA[31] (non-compliant)	Asymmetric Key Generation; Digital Signature Generation
DSA PQG (non-compliant)	Digital Signature Generation
RSA (non-compliant)	Digital Signature Generation (key sizes < 2048)
SHA-1 (non-compliant)	Digital Signature Generation

[28] ECDH – Elliptic Curve DH
[29] HDKF – HMAC-based extract-and-expand Key Derivation Function
[30] J-PAKE – Password Authenticated Key Exchange by Juggling
[31] DSA – Digital Signature Algorithm

2.7.3 Critical Security Parameters

The module supports the CSPs listed below in Table 7.

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation[32] / Input	Output	Storage	Zeroization	Use
AES key	AES128-, 192-, 256-bit key	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Encryption, Decryption
TDES key	TDES 192-bit secure key	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Encryption, decryption
RSA private key	RSA 1024-, 1536-, 2048-, 3072-, 4096-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature generation, unwrapping
RSA public key	RSA 1024-, 1536-, 2048-, 3072-, 4096-bit key	Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature verification, wrapping
DSA private key	DSA 160-bit key	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature generation

[32] The module complies with IG 7.8 Scenario 1 for symmetric key generation as well as the seed supplied to the algorithm for generating asymmetric keys

Key	Key Type	Generation[32] / Input	Output	Storage	Zeroization	Use
DSA public key	DSA 1024-bit key	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Signature verification
DH private keys	DH 160- and 224-bit keys	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Key exchange
DH public keys	DH 1024-, 1536-, and 2048-bit keys	Internally Generated via approved DRBG; or Input via API in plaintext	Output in plaintext via Tested Platform's INT Path	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Key exchange
HMAC Key	HMAC key	Internally Generated via approved DRBG; or Input via API in plaintext	Never	Keys are not persistently stored by the module	Reboot OS; API call; Cycle host power	Message Authentication with SHS
DRBG seed	880-bit random value	Generated Within the Physical Boundary; Input Electronically	Never	The DRBG seed is not persistently stored by the module	Reboot OS; API call; Cycle host power	Seed input to SP 800-90 Hash_DRBG
Hash DRBG V value	Internal hash DRBG state value	Internally generated	Never	DRBG internal values are not persistently stored by the module	Reboot OS; API call; Cycle host power	Used for SP 800-90 Hash_DRBG

Key	Key Type	Generation[32] / Input	Output	Storage	Zeroization	Use
Hash DRBG C value	Internal hash DRBG state value	Internally generated	Never	DRBG internal values are are not persistently stored by the module	Reboot OS; API call; Cycle host power	Used for SP 800-90 Hash_DRBG

2.8 Self-Tests

Cryptographic self-tests are performed by the module after the module begins normal operation as well as when a random number or asymmetric key pair is created. The following sections list the self-tests performed by the module, their expected error status, and error resolutions.

2.8.1 Power-Up Self-Tests

Power-up Self-tests are automatically performed by the module when the module begins normal operation. 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 to the IPSec Service 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 cryptographic self-test error, the module must be restarted by rebooting the Operating System. If the error persists, the module must be reinstalled.

The VMware NSS Cryptographic Module performs the following Power-up Self-tests:

- Software integrity check (DSA 1024-bit Signature Verification)
- Known Answer Tests (KATs)
    - AES KAT (Encrypt)[33]
    - AES KAT (Decrypt)[31]
    - Triple-DES KAT (Encrypt)
    - Triple-DES KAT (Decrypt)
    - RSA KAT (Signature Generation)
    - RSA KAT (Signature Verification)
    - RSA KAT (Wrap)
    - RSA KAT (Unwrap)
    - SHA-1, SHA-256, SHA-384. SHA-512 KAT
    - HMAC SHA-1, SHA-256, SHA-384, SHA-512 KAT
    - SP 800-90A Hash_DRBG KAT
- DSA Pairwise Consistency Test

2.8.2 Conditional Self-Tests

Conditional self-tests are performed by the module whenever a new random number is generated or when a new RSA key pair is generated. If an error is encountered, the module will return an error to the IPSec Service 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 cryptographic self-test error, the module must be restarted by rebooting the Operating System. If the error persists, the module must be reinstalled.

The VMware NSS Cryptographic Module performs the following conditional self-tests:

- SP 800-90A Hash_DRBG Continuous RNG Test
- RSA PCT[34] for key pair generation
- DSA PCT for key pair generation

[33] The module will determine if it is running on an AES-NI supported processor and run the KAT accordingly
[34] PCT – Pairwise Consistency Test

2.8.3 Critical Functions Tests

The SP 800-90A Hash_DRBG employed by the cryptographic module includes four critical functions. These critical functions include instantiation, generation, reseed, and uninstantiation. Each function is tested by the module during the module's power-up self-tests. If any of the self-tests fail, the module will return an error to the IPSec Service 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 cryptographic self-test error, the module must be restarted by rebooting the Operating System. If the error persists, the module must be reinstalled.

The VMware NSS Cryptographic Module performs the following critical functions tests:

- DRBG Instantiate Critical Function Test
- DRBG Generate Critical Function Test
- DRBG Reseed Critical Function Test
- DRBG Uninstantiate Critical Function Test

2.9 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

3 Secure Operation

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

3.1 Crypto Officer Guidance

Installation and operation of the VMware NSS Cryptographic Module requires the proper installation of the vShield Edge Virtual Appliance. The sections below provide a brief summary of the installation procedures for vShield Edge. For a more comprehensive instruction set, please refer to the *vShield Installation and Upgrade Guide* provided by VMware. The VMware NSS Cryptographic Module operates in the FIPS-Approved mode of operation after the instructions for Initial Setup (3.1.1) and Secure Installation (3.1.2) are followed.

All guides mentioned within in these instructions are freely available for download at http://www.vmware.com. These instructions assume that the CO is familiar with VMware vSphere 5.5 and VMware vShield 5.5 products.

3.1.1 Initial Setup

Prior to the secure installation of the vShield Edge Virtual Appliance, the CO shall prepare the virtual environment required to securely operate the virtual appliance. This includes installing the latest version of VMware vSphere 5.5 (see *vSphere Installation and Setup*). Included in this installation is the VMware vSphere Hypervisor (ESXi) 5.5, the vSphere 5.5 vSphere Client, and the vSphere 5.5 vCenter Server, all of which are prerequisites to installing the vShield Edge Virtual Appliance.

After installing the VMware vSphere 5.5 virtual environment, the CO shall log into the vCenter Server using the vSphere Client and follow the instructions provided in Chapter 3 of *vShield Installation and Upgrade Guide* to securely install and configure VMware vShield Manager Virtual Appliance, the management component needed to install vShield Edge.

3.1.2 Secure Installation

In order to install the VMware NSS Cryptographic Module, the CO shall follow the installation instructions provided in Chapter 4 of *vShield Installation and Upgrade Guide* in order to securely install and configure the vShield 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 Wizard”
- Follow the step-by-step instructions of the “Add Edge Wizard” to place the Edge Appliance into FIPS mode
- Add an Edge Appliance
- Confirm the settings and install

Successful completion of installing a vShield Edge Virtual Appliance will be indicated by the appearance of a vShield Edge Virtual Appliance on the ESXi host which the CO specified. Using the vSphere Client, the CO can determine that the virtual appliance is operational. Troubleshooting is available in *vShield Installation and Upgrade Guide*.

3.1.3 VMware NSS Cryptographic Module Secure Operation

Following the successful installation of the vShield Edge Virtual Appliance, the CO shall power on the virtual appliance. Enabling the IPsec Services will power on the VMware NSS Cryptographic Module. After following the steps outlined in Sections 3.1.1 and 3.1.2, the vShield Edge Virtual Appliance will use

the VMware NSS Cryptographic Module for operation in the FIPS-Approved mode. The CO shall follow the guidelines in Chapter 9 of the *vShield Administration Guide* in order to securely configure and operate the VMware NSS Cryptographic Module. Additionally, the CO shall ensure the module is operated in accordance with the transition rules specified in SP 800-131A. Furthermore the transition tables available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/) can be referenced to inform users of the risks associated with using a particular algorithm and a given key length.

3.2 User Guidance

The VMware NSS Cryptographic Module is designed for use by VMware security products. 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 4. The user is responsible for reporting to the CO if any irregular activity is noticed.

4 Acronyms

Table 8 describes the acronyms used in this Security Policy.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
BIOS	Basic Input/Output System
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie Hellman
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
ECB	Electronic Code Book
ECDH	Elliptic Curve DH
ECDSA	Elliptic Curve DSA
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HDD	Hard Disk Drive
HKDF	HMAC-based extract-and-expand Key Derivation Function
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
J-PAKE	Password Authenticated Key Exchange by Juggling
KAT	Known Answer Test
KO	Keying Option

Acronym	Definition
LCD	Liquid Crystal Display
LED	Light Emitting Diode
NAT	Network Address Translation
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PCI(e)	Peripheral Component Interconnect (express)
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
RAM	Random Access Memory
RC	Rivest Cipher
RSA	Rivest Shamir Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Security Policy
TCP	Transmission Control Protocol
TDEA	Triple Data Encryption Algorithm
UDP	User Datagram Protocol
USB	Universal Serial Bus
VNCM	VMware NSS Cryptographic Module
VPN	Virtual Private Network

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