NitroView Enterprise Security Manager
Version 8.0.0.20080605
Security Policy

FIPS 140-2 Level 2 Validation

Model Numbers
NS-ESM-4245-R
NS-ESMR-4200-R
NS-ESM-5750-R

March 16, 2009
Version 1.17

1 Introduction

This document is the Security Policy for NitroSecurity NitroView Enterprise Security Manager (ESM) cryptographic module. This Security Policy specifies the security rules under which this cryptographic module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the NitroView ESM cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to the FIPS 140-2 standard. The Cryptographic Algorithm Validation Program (CAVP) validates algorithms used by a FIPS validated module. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard, and information on the CMVP can be found at http://csrc.nist.gov/groups/STM/cmvp. Information on the CAVP can be found at http://csrc.nist.gov/groups/STM/cavp. More information describing the NitroView ESM can be found at http://www.NitroSecurity.com.

In this document, the NitroSecurity NitroView Enterprise Security Manager is also referred to as “the NitroView ESM”, “the ESM”, or “the module”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “NitroSecurity - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The NitroSecurity NitroView ESM cryptographic module meets the overall requirements applicable to Level 2 security for FIPS 140-2 as shown in Table 1.

Table 1. Cryptographic Module Security Requirements.

Security Requirements Section	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	NA
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Cryptographic Module Security Policy	2

Document Version History

Version	Date	Comments	Name
1.00	4/3/08	Initial Draft	Ward Rosenberry
1.02	5/8/08	Completed Draft2	Ward Rosenberry
1.03	6/5/08	Trial Submission Draft	Ward Rosenberry
1.04, 1.05,		Internal Versions	Ward Rosenberry
1.06	7/16/08	Resubmitted	Ward Rosenberry
1.07	7/31/05	Responded to evaluator comments	Ward Rosenberry
1.08	8/19/08	Responded to 2nd round evaluator comments	Ward Rosenberry
1.09, 1.10	9/15/08, 10/13/08	Evaluator comments	Ward Rosenberry
1.11	12/23/08	Updated FIPS mode vs non-FIPS and PRNG seed key information	Bill Virtue
1.12 / 13	1/14/09	Changes to table 8 & 9 per CSE (Canada)	Bill Virtue
1.14	2/11/09	Changes to section 2.2,4.1.6, table 5 & table 10 per CSE (Canada) – see change order saic_262009	Bill Virtue
1.15	3/11/09	Changes to section 7, 8, and 9	Bill Virtue

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
DH	Diffie-Hellman Algorithm
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication

RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman public key cryptosystem
SHA-1	Secure Hash Algorithm
SHA-384	Secure Hash Algorithm
T-DES	Triple-DES (Data Encryption Standard)

2 NitroSecurity NitroView ESM

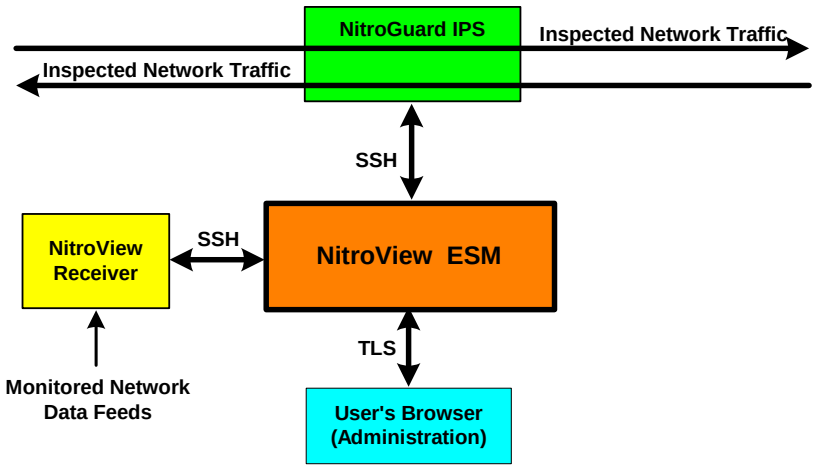
2.1 Functional Overview

NitroSecurity provides highly scalable enterprise security solutions that provide intrusion prevention, network behavior analysis and security event management enabling enterprises to secure their networks with real-time threat mitigation.

The NitroView Enterprise Security Manager (ESM) is unique due to a patented, ultra-high-performance aggregation and correlation engine that is integrated into each NitroView ESM. These sophisticated data acquisition and management capabilities give the NitroView ESM the power to manage thousands of events per second. The NitroView ESM provides advanced correlation and analysis of relevant security information collected from IDS, IPS, firewalls, servers, hosts, and many other devices. By unifying relevant security information, NitroView is able to provide Unified Security Management (USM), combining and enhancing security event management (SEM), security information management (SIM), network behavior analysis (NBA), and anomaly detection functions. The NitroView ESM uses an advanced, highly responsive web-based Graphical User Interface (GUI) to provide near real-time analysis and reporting of both live data (events as they're acquired) and deep forensics (events collected over months or years).

Figure 1 shows a high level functional view of the NitroView ESM. The NitroView ESM uses data acquired by NitroView Receiver and NitroGuard IPS devices to provide data for its correlation and analysis capabilities. Users access all NitroView ESM, NitroView Receiver and NitroGuard IPS devices via an encrypted HTTPS communication channel between their browser and the NitroView ESM's embedded web server. All communication between the NitroView ESM and the NitroView Receiver and NitroGuard IPS devices (i.e. Commands and data) uses an encrypted SSH connection. Data collection, correlation and analysis features are available for security events and network flows provided by a NitroGuard IPS device.

Figure 1. Functional View of the Cryptographic Module.



2.2 Module Description

The NitroSecurity NitroView ESM is a multi-chip standalone cryptographic module consisting of production-grade components contained within an opaque hard production-grade enclosure (the outside case is steel). The removable cover is protected by tamper evident security seals in accordance with FIPS 140-2 Level 2. The cryptographic boundary is the metal enclosure of the device. The module has a single processor complex, composed of one or more CPUs each with one or more general purpose CPU cores, and all of the module services implemented by module software are executed by this processor complex, using the memory devices that contain the executable code and data. Note that all of the CPU cores in the processor complex are general purpose, and none of them have any FIPS security relevant functionality implemented in hardware.

The module is available in the following functionally identical physical configurations:

- The NS-ESM-4245-R uses a 2U chassis that supports up to four hard disk drives for data storage.
- The NS-ESMR-4200R consists of exactly the same hardware and software as the NS-ESM-4245-R but has a different part number for ordering purposes.
- NS-ESM-5750-R uses a 3U chassis that supports up to 12 hard disk drives for data storage. .

The module has a limited operational environment and does not have a FIPS bypass mode or a FIPS maintenance mode.

The NitroView ESM meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, for Class B devices.

The module uses algorithms from OpenSSL that is built, installed, protected and initialized as specified in the *OpenSSL FIPS 140-2 Security Policy* Version 1.1.2, dated January 29, 2008. Appendix B of the OpenSSL Security Policy specifies the complete set of source files of this module. There are no additions, deletions or alterations of this set as used during module build. All source files, including the specified OpenSSL distribution tar file, are verified as specified in Appendix B of the OpenSSL Security Policy. Installation, protection, and initialization must be completed as specified in Appendix C of the OpenSSL Security Policy. That information is available to consumers of the ESM cryptographic module. Any deviation from specified verification, protection, installation and initialization procedures will result in a non FIPS 140-2 compliant module.

Once the software is installed there are no modifications allowed to the OpenSSL or OpenSSH software components. NitroSecurity Linux kernel version 2.6.18.5 is unlikely to be modified.

2.3 Module Ports and Interfaces

The cryptographic module has numerous physical ports and four logical FIPS 140-2 interfaces. The physical ports are described in Table 2.

Where distinct logical interfaces share the same physical port, communication protocols (such as TCP/IP, and 802.3) and the ESM application rules of operation logically separate and isolate these interfaces from one another.

Table 2. Physical Ports Descriptions.

Physical Port	*Description*
Front Panel	
Power On Switch	Power input
Power Off Switch	Power input
Arrow Keys	Control input
LCD Display	Status output

Physical Port	Description
Rear Panel	
Management Port 1	Network interface card connector for control input, status output, data input and data output. The network interface card may support an RJ45 copper interface (10/100/1000 megabit). This port may connect to a management browser and external IPS and Receiver devices.
Management Port 2	Network interface card connector with the same functionality as Management Port 1. The ESM may use this as an alternate management port and may connect to a management browser and external IPS and Receiver devices.
VGA Monitor Port	15-pin D-connector for status output.
Serial Port	Not used.
Mouse Port	PS2 Control input from mouse.
Keyboard Port	PS2 Control input from keyboard.
USB 0	Not used
USB 1	Not used
Power Input 1	This is not a FIPS 140-2 logical interface. Power (110 / 220 VAC) enters the module via the power input connectors.
Power Input 1 LED	Green indicates power is available to the module via this power connector. Yellow indicates power is not available at this power connector. Unlit indicates no power is connected to this power connector.
Power Input 2	This is not a FIPS 140-2 logical interface. Power (110 / 220 VAC) enters the module via the power input connectors.
Power Input 2 LED	Green indicates power is available to the module via this power connector. Yellow indicates power is not available at this power connector. Unlit indicates no power is connected to this power connector.
UID Switch	Pressing this switch enables the front LED to identify the unit in a rack of devices. This non-security relevant switch is not available on all ESM models.

The FIPS 140-2 logical interfaces correspond to physical ports as described in Table 3.

Table 3. FIPS 140-2 Logical Interfaces.

Logical Interface	Description
Data input	Data input consists of: • encrypted metadata entering the cryptographic module via Management Port 1 over an SSH connection from IPS and Receiver devices for the purpose of being analyzed and/or archived.

Logical Interface	Description
Data output	Data output consists of: • encrypted event analysis (instrumentation) data exiting the cryptographic module via Management Port 1 or Management Port 2 to a browser over an HTTPS connection. • encrypted commands exiting the cryptographic module via Management Port 1 or Management Port 2 over an SSH connection for the purpose of controlling an IPS or Receiver device. • plaintext data event analysis data exiting the cryptographic module via Management Port 1 or Management Port 2 over a TCP/IP socket connection for the purpose of being stored in an external event storage system.
Control input	Control input consists of: • commands from crypto officers and users entering the module from a browser in encrypted format via Management Port 1 or Management Port 2 over an HTTPS connection. • commands from crypto officers entering the module via the keyboard and mouse ports and the arrow keys on the front of the system
Status output	The status output consists of • FIPS operational status returned from status requests by crypto officers. FIPS operational status is output in encrypted format on the HTTPS (browser) connection. The ESM system properties dialog displays the result of the most recent FIPS self-test. • FIPS error status output automatically in plaintext format to the LCD and on HTTP port 4242 (management ports 1 and 2). The power inputs LEDs also indicate status of power supplied to the module.

3 Security Functions

The NitroView ESM cryptographic module implements the security functions described in Table 4.

Table 4. Module Security Functions.

Security Function	Purpose or Use	Certificate
Approved Security Functions		
AES (FIPS PUB 197) CBC(e/d; 128, 256)	TLS encryption and decryption (256) and SSH encryption and decryption (128).	668
Triple-DES (FIPS PUB 46.3)	Support for ANSI X9.31 PRNG	613
SHA-1 (FIPS PUB 180-2) (BYTE-only)	TLS and SSH signature verification, data integrity	701
HMAC-SHA1	Data integrity and data authentication within SSH	352 (HMAC), 701 (SHS)
RNG (ANSI X9.31 PRNG, Appendix A.2.4)	Key generation	387

Security Function	Purpose or Use	Certificate
RSA (FIPS PUB 186-2) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048, SHS: SHA-1	TLS and SSH key transport, signature verification	310
Allowed Security Functions		
Diffie Hellman (2048 bit key agreement and key establishment methodology). While not approved, it may be used in FIPS mode.	Key agreement within SSH	N/A

4 FIPS Approved Mode of Operation

The Master Crypto Officer must select FIPS mode during initial configuration. Once in FIPS mode the module performs only FIPS-approved cryptographic algorithms and security functions. The module can not allow a NitroGuard IPS and/or NitroView Receiver to communicate and become registered until they have been configured in a FIPS approved mode of operation.
In the FIPS approved mode, crypto officers may configure the module for operation within the IT environment and are able to perform administrative changes. Users of the module are defined to be either a NitroGuard IPS or NitroView Receiver. The module allows loading software updates in the field, but this operation must not be used as this operation invalidates the module's FIPS evaluated configuration.

The module supports a non-FIPS mode of operation. If during initial configuration the Master Crypto Officer does not enable FIPS mode, the module will not be in FIPS mode and can only communicate with a non-FIPS mode ESM. There is a Non-FIPS mode communication between the NitroGuard IPS, NitroView Receiver and the module, however, this is considered proprietary.

The module supports protocols and functionality that are used within the approved FIPS 140-2 mode of operation and non-approved FIPS 140-2 mode of operation:

FIPS Approved Mode of Operation: HTTPS (TLS 1.0), OpenSSH (using FIPS-approved cryptographic algorithms and security functions).

Non-FIPS Approved Mode of Operation: SNMP V3, OPSEC (Operations Security), plaintext.

4.1 Set-Up and Initialization Procedures

The NitroSecurity Operator Guidance provides the following steps to set up and initialize the module into FIPS mode:

1. Check the packaging and the module, including the two tamper evident seals for signs of tampering. If tampering is detected, contact NitroSecurity Support for instructions. Place the third tamper-evident seal so it covers the USB ports. This seal can be found in the package of accessories included in the shipping container.
2. Power up the module.
3. After the module boots up, configure the network interface by following the instructions in the *NitroSecurity Installation and Setup Guide* section "Configuring the Network Interface on the ESM".
4. Use a browser to log into the ESM following the instructions in the *NitroSecurity Installation and Setup Guide* section "Logging Into NitroView". Change the default password as instructed.
5. When the module prompts to choose FIPS approved mode or non-approved mode, choose FIPS approved mode. The module configures itself for permanent operation in FIPS approved mode.

6. To verify FIPS mode use the NitroView ESM GUI. The bottom 'status' bar indicates that the module is in FIPS mode (shows version / date and "FIPS Enabled"). Using the GUI, select a single device go to device properties, click the FIPS button – runs the FIPS self test and outputs the FIPS status
    a. Additionally, the master crypto officer is able to see the FIPS status when they authenticate to cryptographic module's console. The FIPS status can be observed when the crypto officer selects the command line option number 3 to determine whether the cryptographic module is in a FIPS approved mode of operation.

At this point the ESM is fully configured. You may proceed to establish communications with managed IPS and Receiver devices by using the ESM management interface to key those devices.

If the Test Failed condition "0" (a single ASCII zero) is displayed, reboot the ESM to try and correct the problem. If the Test Failed condition persists, contact NitroSecurity Support for further instructions. If the FIPS Status web page returns a single "1", a single ASCII one, then the module is in proper FIPS operating condition.

If you are instructed to return the ESM to the factory, be sure to zeroize the encryption keys by giving the "Prepare unit for RMA" command on the console. After zeroization is complete you can return the device to NitroSecurity.

5 Identification and Authentication

The module supports two crypto officer roles and user roles. See section [7 Roles and Services

Formatted: Bullets and Numbering

The module supports a master crypto officer role, a crypto officer role and user roles. The module has a single system administrator role that is designated as the master crypto officer role and that role has the user name "root". The master crypto officer role may initialize the module using the LCD and front panel controls, may zeroize the module using the console port, and perform other operations unique to the role. Crypto officers access the device over the SSH channel, give commands to use the ESM device features, and perform key management operations, all of which are referred to as the "ESM Instrumentation" in table 8 below.

The module supports services that are available to module operators in the various roles. All of the services are described in detail in the module's user documentation. Table 8 shows the services available to the various roles.

Multiple concurrent role-based sessions (crypto officer and user roles) are allowed. The module's "System Administrator, which always has the master crypto officer role, is the only user that can give or revoke a user's crypto officer role, and can do so at any time, even during a user's session after the user has authenticated. Separation of roles is achieved by first requiring authentication before granting access to services offered to a particular role. The software then programmatically separates roles and services during module use by providing role-specific services to the specific authenticated role. The software programmatically separates concurrent sessions within a role through the use of atomic operations for all operations that change configuration data. The event logging system records all access to the system and associates all configuration changes with the identity of the session making the change. Roles cannot be changed while authenticated to the module.

The module does not display any authentication data or feedback data entered into the module console port. Black dot feedback characters indicating a key was pressed are returned when authenticating to the HTTPS management interface. Access to the authorized roles is restricted as explained in Table 5:

Table 5. Roles and Required Identification and Authentication.

Role	*Type of Authentication*	*Authentication Data*
Master Crypto Officer	Role-based	A master crypto officer authenticates by entering a username and a password at the console. Start-up and other operations using the LCD and front panel arrow controls are unauthenticated.

Role	Type of Authentication	Authentication Data
Crypto Officer	Role-based	A crypto officer authenticates by entering a user name and a password.
User	Role-based, Identity-based	A user authenticates by entering a user name and a password to the module. NitroGuard IPS and NitroView Receiver are considered users since an ESM communicates with these devices. Authentication is performed via public key authentication.

The strength of the operator authentication, per the above roles, is as follows in Table 6:

Table 6. Strength of Authentication.

Authentication Mechanism	Strength of Mechanism
Password	"The master crypto officer, crypto officers, and users authenticate using a minimum 8 ASCII-character (Decimal values between 33 and 126, inclusive) password that must include all of the following: one upper case character (A-Z), one digit (0-9), and one special character (printable characters excluding space and alphanumerics, 32 choices). This yields a minimum of 61.1E+12, over 61 trillion, possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000.. The possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. The system allows no more than 6,000 login attempts per minute. Combine this fact with a one in 61 trillion possibility of guessing a password to compute only a 1 in 10.2E+9, over 10 billion, possibility of guessing a password in one minute."
Public key authentication	The ESM supports public key based authentication with RSA 2048-bit keys. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000. The possibility of randomly guessing a key in 60 seconds is less than 1 in 100,000. The system allows no more than 6,000 login attempts per minute. Combine this fact with a one in 61 trillion possibility of guessing a password to compute only a 1 in 10.2E+9, over 10 billion, possibility of guessing a password in one minute.

When the cryptographic module is powered off and subsequently powered on, the results of previous authentications (the authentication states of sessions) are cleared from memory. When the module is powered up again, operators must re-authenticate, entering the correct user name and password.

6 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module. Cryptographic keys and CSPs are never output from the module in plaintext. An Approved key generation method is used to generate keys that are generated on the module. Cryptographic keys in the section of the table labeled Other Cryptographic Keys are not considered CSPs as they are public keys.

Table 7. Cryptographic Keys and CSPs.

Data Item	Description
HTTPS Private Key	RSA 2048-bit private key used for the symmetric key wrapping in the Web administration interface (TLS). The key is generated by the FIPS validated RNG (certificate # 387) at intervals defined by the organization's security policy, or the master crypto officer can import a validated key (pair). The key is stored in unencrypted format on an unencrypted disk partition. The key is zeroized according to DoD 5220.22-M[1] on a rekey or when returning the module to the manufacturer for repair or replacement.
Default SSH Private Key	RSA 2048-bit private key used for the transfer of key material in the SSH protocol. The key is generated off the module and are stored in unencrypted form in the file system on an unencrypted disk partition. After module initialization, this key is maintained on the module for initial authentication with new devices added to the system.
Active SSH Private Key	RSA 2048-bit private key used for the transfer of key material in the SSH protocol. The key is generated by the FIPS validated RNG (certificate #387) during manufacturing. The key is stored in unencrypted format on an unencrypted disk partition. The key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
TLS AES Encryption Keys	AES 256-bit ephemeral symmetric key used for encrypting and decrypting TLS sessions for the Web administration interface. This key is produced using DH key agreement. The key is deleted from memory after use.
SSH AES Encryption Keys	AES 128-bit ephemeral symmetric key used for encrypting and decrypting SSH sessions with IPS and Receiver devices. This key is produced using DH key agreement. The key is deleted from memory after use.
Diffie-Hellman Keys	Ephemeral Diffie-Hellman public and private parameters used for key agreement to provide SSH AES Encryption Keys. These key parameters are deleted from memory after use.
HMAC Key	The ephemeral HMAC key is used within the SSH protocol for data authentication purposes. It is generated as specified in the SSH protocol specification [2] (using OpenSSH). This key is deleted from memory after use.
Default Crypto Officer Password	An 11-character password used by crypto officers to authenticate to the Web Administration interface for module initialization purposes only. As soon as the master crypto officer logs in using this password, the module forces the master crypto officer to set another password. An obfuscated, non-human readable but not encrypted, version of the password is stored in the file system on an unencrypted disk partition.
Master Crypto Officer Password	A minimum 8-character password used by the master crypto officer to authenticate to the Web Administration interface. The master crypto officer sets his or her own password that is associated with the user name NGCP. An obfuscated, non-human readable but not encrypted, version of the password is stored in the file system. The limited operating environment does not provide access to operating system services to access the obfuscated password data. This password is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.

[1] http://www.dtic.mil/whs/directives/corres/html/522022m.htm

[2] http://www.ietf.org/rfc/rfc4252.txt

Data Item	Description
Crypto Officer Password	A minimum 8-character password used by crypto officers to authenticate to the Web Administration interface. Each crypto officer has his or her own password that is associated with a user name. An obfuscated, non-human readable but not encrypted, version of the password is stored in the file system. The limited operating environment does not provide access to operating system services to access the obfuscated password data. This password is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
User Passwords	A minimum 8-character password used by operators to authenticate to the Web Administration interface. Each operator has his or her own password that is associated with a user name. An obfuscated, non-human readable but not encrypted, version of the password is stored in the file system. The limited operating environment does not provide access to operating system services to access the obfuscated password data. This password is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Seed Key	Triple DES 168 bit seed key used to initialize the ANSI X9.31 Pseudo RNG which is used to generate other cryptographic keys.
RNG Seed	OpenSSL uses /dev/random as a source of random numbers. The linux kernel initializes this pseudo device at system startup. /dev/random guarantees a high degree of entropy and blocks until it has the proper level of entropy. The FIPS-validated version of OpenSSL performs continual tests on the random numbers it uses.
Other Cryptographic Keys	
HTTPS Public Key	This RSA 2048-bit public key corresponds to the HTTPS Private Key described above. This public key is output from the module in plaintext form as it is used for the transfer of key material in the SSH protocol. This key is generated by the FIPS validated RNG (certificate #387) at intervals defined by the organization's security policy, or the master crypto officer can import a validated key (pair). The key is stored in unencrypted format on an unencrypted disk partition. The public key is maintained in a self signed certificate by default, but may be signed by a certificate authority if a key pair is imported. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.
Default SSH Public Key	This RSA 2048-bit public key corresponds to the Default SSH Private Key described above. RSA 2048-bit public key used for the transfer of key material in the SSH protocol. This key is generated off the module and is stored in unencrypted form in the file system on an unencrypted disk partition. After module initialization, this key are maintained on the module for initial authentication with new devices added to the system.
Active SSH Public Key	This RSA 2048-bit public key corresponds to the Active SSH Private Key described above. RSA 2048-bit public key pair used for the transfer of key material in the SSH protocol. This key is generated by the FIPS validated RNG (certificate #387) during manufacturing. The key is stored in unencrypted format on an unencrypted disk partition. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.

Data Item	Description
Software Integrity Public Key	RSA 2048-bit public key used to verify the digital signature of stored hash values used for the software/firmware integrity test. The public key is generated off the module and is maintained in a self signed certificate stored in unencrypted form in the filesystem. This key is zeroized according to DoD 5220.22-M when returning the module to the manufacturer for repair or replacement.

7 Roles and Services

The module supports a master crypto officer role, a crypto officer role and user roles. The module has a single system administrator role that is designated as the master crypto officer role and that role has the user name ”root”. The master crypto officer role may initialize the module using the LCD and front panel controls, may zeroize the module using the console port, and perform other operations unique to the role. Crypto officers access the device over the SSH channel, give commands to use the ESM device features, and perform key management operations, all of which are referred to as the “ESM Instrumentation” in table 8 below.

The module supports services that are available to module operators in the various roles. All of the services are described in detail in the module’s user documentation. Table 8 shows the services available to the various roles.

Table 8. Roles and Services

Service	Master Crypto Officer	Crypto Officer	User
Change password, Authenticate to Console Interface, Initialize ESM, Key ESM, Start system, Zeroize system	●		
Import Device Keys, ESM Instrumentation, Reboot system, Rekey ESM, Shutdown system	●	●	
Read Status via HTTPS (Show Status)	●	●	
Read Status via HTTP (port 4242)	●	●	
Read Status via Console (Show Status)	●		
Read FIPS self-test (Reboot and On Demand)	●	●	
Authenticate to ESM			●

Importing Device Keys is available as part of the NitroGuard IPS and/or NitroView Receiver registration process to the ESM crypto module. This registration is performed by exchanging ‘key’ information. A unique key is assigned to a NitroGuard IPS and/or NitroView Receiver for the purpose of identifying it as a valid device. Keying the device enables the ESM to communicate with the NitroGuard IPS and/or NitroView Receiver and ensures added security by ignoring all outside sources of communication.

Note: A key exported from a non-FIPS device cannot be imported to a device operating in

FIPS mode, nor can a key exported from a FIPS device be imported to a non-FIPS device. If you attempt to perform this action when you are adding a device to the system, the “The file is invalid” error will appear.

This term ‘Key’ in this manner is not related to encryption keys and refers to device registration keys.

NitroSecurity uses the Linux ‘shred’ command as the actual ‘process’ to securely erase disk data following the guidelines under the authority of DoD Directive 5220.22-M for the protection of classified information. NitroSecurity also recommends its customers become familiar with the NIST Special Publication 800-88 (Guidelines for Media Sanitation) to devise an appropriate erasure policy specific to their environment.

The Linux ‘shred’ command is designed primarily to securely delete files on the system. Using ‘shred’ overwrites all addressable hard drive locations with a character, its complement, and then a random character, followed by verification. The procedure is completed a number of times and prevents data from being recovered by commercially available processes.

8 Access Control

Table 9 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is read or referenced by the service.
W - The item is written or updated by the service.
E - The item is executed by the service. (The item is used as part of a cryptographic service.)
D - The item is deleted by the service.
Z - The item is zeroized (DoD erasure according to DoD 5220.22-M) by the service.

Table 9. Access Control

Key or CSP	*Service*	*Access Control*
Default ESM SSH Public Key, HTTPS Public Key	Initialize ESM	R,E
	Zeroize system	Z
Active ESM SSH Public Key	Key ESM	W,E
	ESM Instrumentation	R,E
	Zeroize system	Z
Default SSH Private Key, Active SSH Private Key, HTTPS Private Key	Rekey ESM	W,E
	ESM Instrumentation	R, E,D
	Import Device Keys	W
	Zeroize system	Z
SSH AES Encryption Key, TLS AES Encryption Key, Diffie-Hellman Keys	ESM Instrumentation	D,W,E
	Shutdown system	D
	Reboot system	D
Default Crypto Officer Password, Crypto Officer Password, User Passwords	Change password	W,D
HMAC Key	ESM Instrumentation	D,W,E
	Shutdown system	D
	Reboot system	D

Key or CSP	Service	Access Control
Integrity Public Key	Start system	E
	Zeroize system	Z
Master Crypto Officer Password	Change password	W,D
	Authenticate to Console Interface	R
	Zeroize system	Z
RNG Seed Key	ESM Instrumentation, Key ESM, Reboot system, Rekey ESM, Shutdown system , Start system, Zeroize system	W,R,E,D

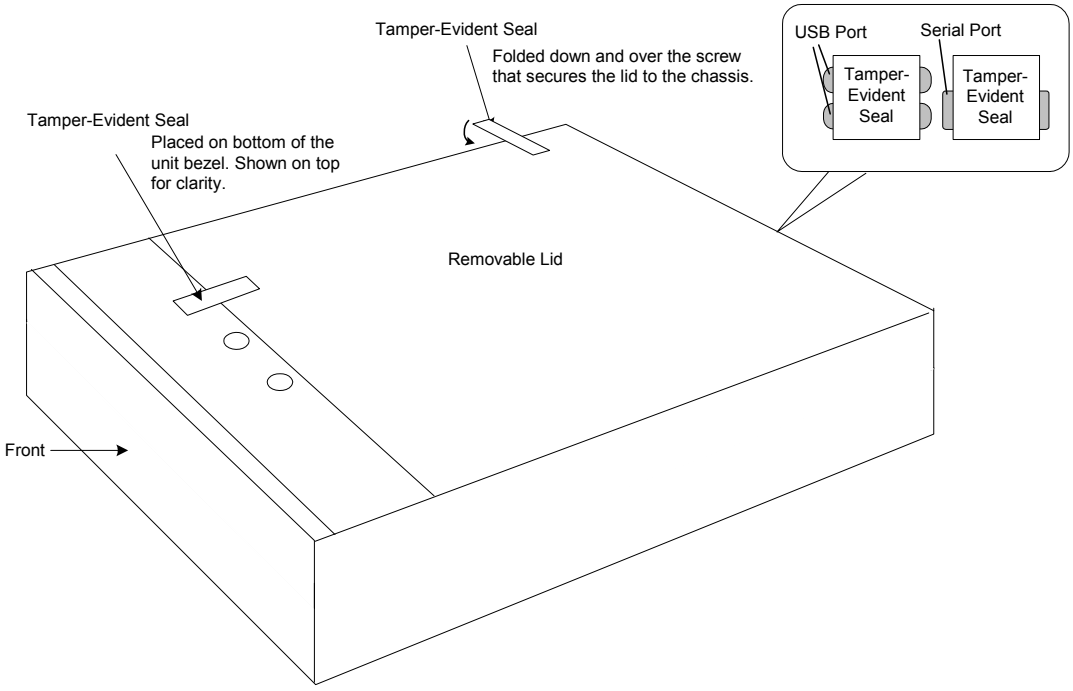
9 Physical Security

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The cryptographic module consists of production-grade components that include standard passivation techniques (a sealing coat applied over the module's circuitry to protect against environmental or other physical damage). The module meets commercial-grade specifications for power, temperature, reliability, shock and vibration.

The module has three tamper-evident seals that are serialized so they can be tracked by the crypto officer. One is placed over the seam where the top removable lid slides forward under the chassis top cover. The second seal is placed over the rear seam between the top cover and the rear panel. The third seal is covering the USB ports on the back of the module. The top cover is removed by sliding it back and then lifting it off. This action breaks both seals, leaving evidence of tampering. The crypto officer guidance directs the crypto officer to periodically inspect the module for signs of tampering such as dents or scratches on the module enclosure or damage to the tamper evident seals. If tampering is detected, the crypto officer is instructed to perform a zeroize command and then to contact NitroSecurity Support for further assistance.

Figure 7 shows how the tamper evident seals are placed over the front and rear seams between the module's removable lid and the module chassis. A crypto officer applies a tamper evident seal (provided with the module) over the USB connectors and another tamper evident seal (also provided with the module) over the serial port to prevent their use without leaving evidence of tampering. These seals must be inspected in accordance with the organization security policy.

Figure 7. Tamper Evident Seals.



10 Self Tests

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating that a failure has occurred and transitions to an error state, blocking all data input, data output and control input via their respective interfaces.

While the module is performing any power on self test or conditional test, software rules within the executable image prevent the module from entering a state where data output via the data output interface is possible.

Anyone with physical or logical access to the module can run the POST on demand by power cycling the module or entering a Reboot command using the keypad. Anyone with logical access to the module, using the GUI, can run the POST on demand by rebooting the device, or just initiating a POST.

Table 10 summarizes the system self tests and conditional tests.

Table 10. Self Tests.

Self Test	*Description*
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, Triple-DES, SHA-1, and RNG) performed by the module, is tested using a "known answer" test to verify the correct operation of the algorithm.
Software Integrity Test	The module verifies the RSA 2048 bit digital signatures on SHA-1 hashes of the NitroSecurity Software (Version 8.0.0.20080605) to confirm their integrity.
Critical Functions tests performed at power-up:	
None	No security-relevant critical functions tests are performed.
Conditional tests performed, as needed, during operation:	
Pairwise Consistency Tests	The module performs pair wise consistency tests whenever RSA asymmetric keys are generated.
Continuous RNG	16 bits continuous testing is performed during each use of the approved RNG. This test is a "stuck at" test to check the RNG output data for failure to a constant value.

Any self test success or failure messages are output to error log files.

Known answer tests for encryption/decryption or hashing, function by encrypting or hashing a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated output does not match the expected value. For decryption, the test then decrypts the ciphertext encrypted string. A decryption test passes when the freshly calculated output matches the plaintext value. A decryption test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

Pair wise consistency tests for RSA keys (these keys are used for key transport) use the public key to encrypt a plaintext value. The resulting ciphertext value is compared to the original plaintext value. If the two values are equal, then the test fails. If the two values differ, the private key is used to decrypt the ciphertext and the resulting value is compared to the original plaintext value. If the two values are not equal, the test fails.

11 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

12 References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: http://csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: http://csrc.nist.gov/groups/STM/cmvp.