Hughes Network Systems, LLC

IPsec IP Gateway Server

Hardware Version: 1507355-8022
IPsec IPGW Firmware Version: 7.4.1.15
Management Gateway Client Firmware Version: 7.4.1.8

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.4

Prepared for:

Hughes Network Systems, LLC
11717 Exploration Lane
German, MD 20876
United States of America

Phone: +1 301 428 5500
www.hughes.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the IPsec IP Gateway Server from Hughes Network Systems, LLC (hereafter referred to as "Hughes"). This Security Policy describes how the IPsec IP Gateway Server meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] 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 Canadian Centre for Cyber Security (CCCS) 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 policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The IPsec IP Gateway Server is referred to in this document as IPsec IPGW, 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 Hughes website (https://www.Hughes.com) contains information on the full line of products from Hughes.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Hughes. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Hughes and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Hughes.

[1] U.S. – United States

2. Hughes IPsec IPGW

2.1 Overview

Hughes is a global leader in broadband satellite technology and managed network services for home and office. Hughes' broadband satellite systems enable operators and enterprises to deliver a comprehensive range of services including broadband Internet access, cellular backhaul, communications on the move, and VoIP[2,3] telephony.

The Hughes JUPITER™ System is a broadband satellite system designed to support high-throughput satellite communications and offers a range of operations for optimized traffic capacity, terminal performance, Gateway (GW) design, and network management. It consists of VSAT[4] satellite terminals, single rack or multi rack JUPITER GWs (facilities used to host the equipment providing uplink and downlink connectivity to the satellite), and the capabilities to manage these devices over the network.

The IPsec IPGW is a JUPITER GW component that can reside either on the JUPITER GW or outside the JUPITER GW in a customer data center. It is used to provide Internet access for associated terminals, perform IP acceleration and routing of packets between terminals and the Internet, and encrypt user traffic between itself and HT Satellite Router terminals via IPsec tunnels. Figure 1 below shows integration of all JUPITER System components.

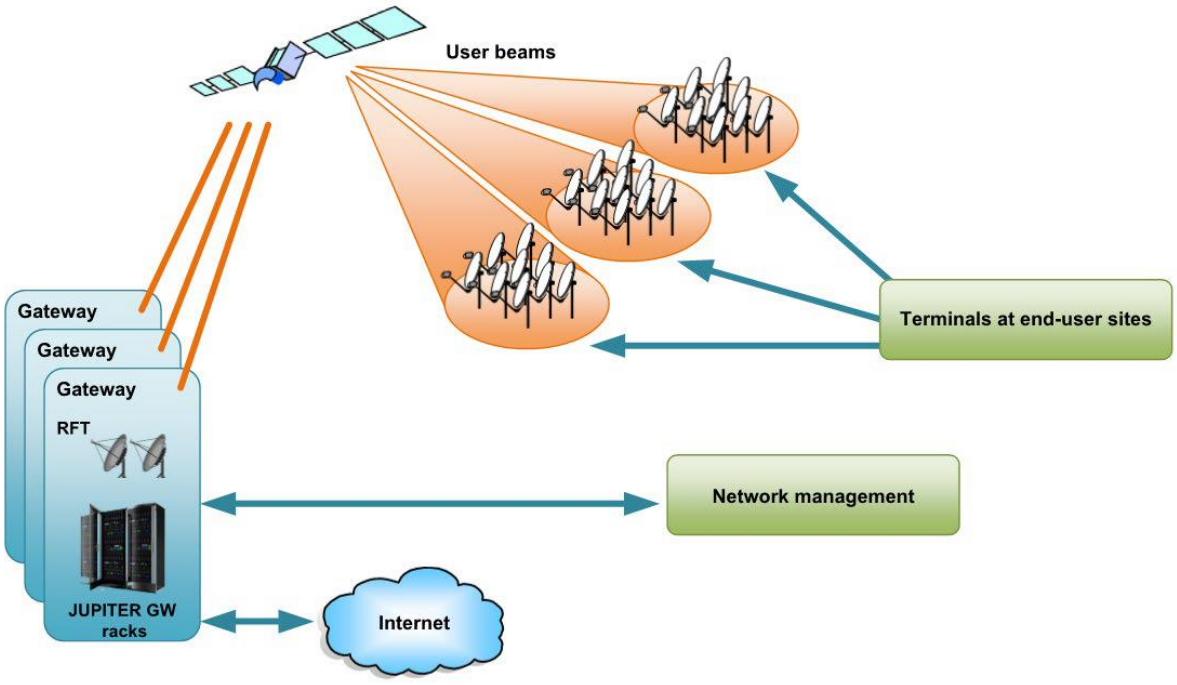

Figure 1 – IPsec IPGW Deployment in Data Center

[2] VoIP – Voice over IP
[3] IP – Internet Protocol
[4] VSAT – Very Small Aperture Terminal

The IPsec IPGW is configured using the external Network Management System (NMS) UI[5]. Configuration files are created by an administrator using the external NMS UI, stored on the NMS Management File Server (MFS), and automatically downloaded over SFTP to the Management Gateway Client (MGC) on the IPsec IPGW appliance.
The prime objective of the Jupiter Management Gateway Client (MGC) application is to deploy, upgrade and manage software components, including executables and configuration files from the Network Management System (NMS) on the target machine.
The configuration files are loaded and used by the IPsec IPGW firmware. Operators view device information, status, and statistics through the IPsec IPGW Web UI.

The IPsec IPGW 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	1
6	Operational Environment	N/A[6]
7	Cryptographic Key Management	1
8	EMI/EMC[7]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The IPsec IPGW is a hardware module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The module consists of hardware and firmware components enclosed in a secure, production-grade metal case. The cryptographic boundary of the IPsec IPGW surrounds the entire enclosure of the server.

The cryptographic module was tested and found compliant on the following platform:

- HPE DL360 Gen10 Server with Intel Xeon-Gold 6230 (2.1 GHz[8]) processor running CentOS 8.2.2004.

The module includes the cryptographic algorithm providers listed in Table 2 below.

[5] UI – User Interface
[6] N/A – Not Applicable
[7] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[8] GHZ – Gigahertz

Table 2 – Cryptographic Algorithm Providers

Certificate Number	Implementation Name and Version	Use
A1457	Hughes IPsec IPGW OpenSSL Crypto Library 1.0	Firmware-based cryptographic primitives (based on OpenSSL 1.1.1c FIPS.
A1458	Hughes IPsec IPGW Kernel Crypto Library 1.0	Kernel-based cryptographic primitives (based on CentOS 8.2.2004 OpenSSL Kernel Crypto)
A1459	Hughes IPsec IPGW IKEv2 Protocol Library 1.0	IKE KDF (based on Hughes proprietary library)

Table 3 below lists all FIPS-Approved algorithms implemented in the Hughes IPsec IPGW Firmware Crypto Library.

Table 3 – Approved Algorithm Certificate Numbers (Hughes IPsec IPGW OpenSSL Cryptographic Library v1.0)

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
A1457	AES[9]	FIPS PUB 197	CBC[10], CTR[11]	128, 256	Encryption/decryption
Vendor Affirmed	CKG[12]	NIST SP 800-133rev2	-	-	Cryptographic key generation *The module generates random strings whose strengths are modified by available entropy.*
A1457	DRBG[13]	NIST SP 800-90Arev1	Hash-based	SHA[14]-256	Deterministic random bit generation
N/A	ENT (P)[15]	NIST SP 800-90B	-	-	Non-deterministic random bit generation
A1457	HMAC[16]	FIPS PUB 198-1	SHA-1, SHA-256	-	Message authentication
A1457	KAS-SSC[17]	NIST SP 800-56Arev3	FFC[18] DH[19] Primitive	Key establishment methodology provides 112 or 150 bits of encryption strength (MODP-2048, MODP-4096)	Shared secret computation *Used in the IKEv2 protocol*

[9] AES – Advanced Encryption Standard
[10] CBC – Cipher Blocker Chaining
[11] CTR – Counter
[12] CKG – Cryptographic Key Generation
[13] DRBG – Deterministic Random Bit Generator
[14] SHA – Secure Hash Algorithm
[15] ENT - Entropy
[16] HMAC – Hash-based Message Authentication Code
[17] KAS-SSC – Key Agreement Scheme Shared Secret Computation
[18] FFC – Finite Field Cryptography
[19] DH – Diffie-Hellman

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
A1457	RSA[20]	FIPS PUB 186-4	PKCS v1.5 SigVer	2048 (SHA2-256)	Digital signature verification *Used in the IKEv2 protocol*
			PKCS v1.5 SigGen	2048 (SHA2-256)	Digital signature generation *Used in the IKEv2 protocol*
A1457	Safe Primes Key Generation	NIST SP 800-56Arev3	Safe Prime Groups: MODP-2048 MODP-4096	2048, 4096	Diffie-Hellman key agreement
A1457	SHS[21]	FIPS PUB 180-4	SHA2-256	-	Message digest

The module includes the following vendor-affirmed security methods in the Hughes IPsec IPGW OpenSSL Crypto Library v1.0:

- *Cryptographic key generation* – As per *NIST SP 800-133rev2*, the module uses the FIPS-Approved Hash-based DRBG specified in *NIST SP 800-90Arev1* to generate random seeds. The resulting generated seeds are unmodified output from the DRBG. The module generates random strings whose strengths are modified by available entropy. According FIPS 140-2 Implementation Guidance D.12, a component key generation (CKG) using the unmodified output of an approved DRBG can be used to generate seed for the asymmetric key generation. This method is valid per option 1 from section "4. Using the Output of a Random Bit Generator" of FIPS SP 800-133rev2. Based on Additional Comments #1 of FIPS IG D.12, this statement is enough and it is not necessary that the vendor justifies the equivalency between this operation and XORing U and V with V as a string of zeros.

The FIPS-Approved algorithms listed in Table 4 below are implemented in the module kernel.

Table 4 – Approved Algorithm Certificate Numbers (Hughes IPsec IPGW Kernel Crypto Library 1.0)

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
A1458	AES	FIPS PUB 197	CBC	256	Encryption/decryption
A1458	HMAC	FIPS PUB 198-1	SHA-1, SHA-256	-	Message authentication
A1458	SHS	FIPS PUB 180-4	SHA-256	-	Message digest

The FIPS-Approved algorithms listed in Table 5 below are implemented in the Hughes IPsec IPGW IKEv2 Protocol Crypto Library 1.0.

Table 5 – Algorithm Certificate Numbers (Hughes IPsec IPGW IKEv2 Protocol Library 1.0)

[20] RSA – Rivest Shamir Adleman
[21] SHS – Secure Hash Standard

Certificate Number	Algorithm	Specification	Mode / Method	Key Lengths / Curves / Moduli	Use
A1459	CVL	NIST SP 800-135rev1	IKEv2	-	Key derivation function *No parts of the IKE protocol, other than the KDFs, have been tested by the CAVP or CMVP.*

The module implements the non-Approved algorithms listed below (these algorithms shall not be used in the Approved mode of operation):

- SNMPv2[22] KDF (non-compliant)

2.2.1 Modes of Operation

The module supports two modes of operation: Approved and non-Approved. The module will be in FIPS-Approved mode when all power up self-tests have completed successfully, and only Approved or Allowed algorithms are invoked. See Table 3, Table 4, and Table 5 above for a list of the Approved and Allowed algorithms.

The module can alternate service-by-service between Approved and non-Approved modes of operation. The module will switch to the non-Approved mode upon execution of a non-Approved service. The module will switch back to the Approved mode upon execution of an Approved service.

The services available in the non-Approved mode of operation are listed in section 2.4 below.

2.3 Module Interfaces

The module's design separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

The cryptographic boundary is defined as the outer casing of the IPsec IPGW. The physical access points on the appliance are the interfaces for the module. Table 6 (front panel) and Table 7 (rear panel) below specify the physical ports and manual controls employed by the module, and provides a mapping from the physical interfaces to logical interfaces as defined by FIPS 140-2.

[22] SNMP – Simple Network Management Protocol

Figure 2 – IPsec IPGW Front Panel

Table 6 – FIPS 140-2 Logical Interface Mappings (Front Panel)

Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
iLO[23] Service Port	1	• Control Input • Status Output
USB[24] 3.0 Port	1	(Not in use)
Power-On Button	1	• Control Input

Figure 3 – IPsec IPGW Rear Panel

Table 7 – FIPS 140-2 Logical Interface Mappings (Rear Panel)

Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
VGA Port	1	• Status Output
Embedded 4x 1 GbE[25] Adapter	1	• Data Input • Data Output
iLO Remote Management Port	1	• Control Input • Status Output
Serial Port	1	(Not in use)
USB 3.0 Port	2	(Not in use)

[23] ILO – Integrated Lights Out
[24] USB – Universal Serial Bus
[25] GbE – Gigabit Ethernet

Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
FlexibleLOM	2	(Not in use)
Power	2	• Power Input

The module uses LEDs[26] to provide status indications for the state and health of the modem. Table 8 below lists each LED and its meaning.

Table 8 – LEDs and Status Indications (Front Panel)

LED Type	Description	FIPS 140-2 Logical Interface

System Power LED	• Solid green – Normal
	• Flashing green – Performing power on sequence
	• Solid amber – System in standby
	• Off – One or more of the following conditions exists:
	  ○ AC power unavailable
	  ○ Power supply failed
	  ○ Power supply in standby mode
	  ○ Power supply exceeded current limit
		• Status output

Health LED	• Red – Critical issue has occurred, and the system is not working properly • Flashing green – iLO is rebooting • Flashing amber – System degraded • Amber – Standby or power is not available • Green – Power is available	• Status output

Table 9 – LEDs and Status Indications (Front and Rear Panel)

LED Type	Description	FIPS 140-2 Logical Interface
UID LED	• Solid blue – Identification is active • Flashing blue – System is being managed remotely • Off – Identification is deactivated	• Status Output
NIC[27] Status LED	• Off – No link to the network • Solid green – Network link • Flashing green – Network link with activity	• Status Output

[26] LED – Light Emitting Diode
[27] NIC – Network Interface Card

2.4 Roles, Services, and Authentication

The sections below describe the module's roles and services and define any authentication methods employed.

2.4.1 Authorized Roles

As required by FIPS 140-2, the module supports two roles that operators may assume: Crypto Officer (CO) role and User role. Each role has access to all module services. Operators implicitly assume the set of both CO and User roles upon accessing the module. The module supports multiple concurrent operators.

2.4.2 Operator Services

Descriptions of the services available to the CO role and User role are provided in Table 10 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

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

Table 10 – Mapping of Module Services to Roles, CSPs, and Type of Access

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Show status	✓	✓	View system status	Command	Status output	None

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Establish IKE/IPsec session	✓	✓	Establish IKE/IPsec session for secure data transmission	Command and parameters	Command response	IKE/IPsec Authentication CA[28] Certificate – R/X IKE/IPsec Authentication Certificate – R/X IKE/IPsec Authentication RSA Private Key – R/X DH Public Key (DH public key component)- R/W/X DH Secret Key (DH private Key component) – R/W/X IKE Shared Secret – W/X IKE Session Key – W/X IKE Authentication Key – W/X IPsec Shared Secret – W/X IPsec Session Key – W/X IPsec Authentication Key – W/X DRBG Entropy – R/X DRBG Seed – R/W/X DRBG 'V' Value – R/W/X DRBG 'C' Value – R/W/X
Create/Change IPsec IPGW Config	✓	✓	Create IPsec IPGW configuration	Command	Command response	None
Display IPsec IPGW Config	✓	✓	View current IPsec IPGW configuration	Command	Command response	None
View IPsec IPGW statistics	✓	✓	View IPsec IPGW statistics to monitor health of the system	Command	Command response	None
Load firmware	✓	✓	Load new firmware into the module while in a FIPS-Approved mode of operation	Command and parameters	Status output	Firmware Verification Key – R/X
Perform self-tests on demand	✓	✓	Perform self-tests on demand by rebooting or power-cycling the module	Command	Status output	Firmware Verification Key – R/X All ephemeral keys – Z
Reboot	✓	✓	Manually reboot and power-cycle the module and perform self-tests on demand	Reset button	Status output	Firmware Verification Key – R/X All ephemeral keys – Z

[28] CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Restart Apps	✓	✓	Perform restart of IP GW application	Command	Status output	All ephemeral keys – Z
Zeroize	✓	✓	Zeroize keys and CSPs	Command	Command response	All ephemeral keys – Z IKE/IPsec Authentication Certificate - Z IKE/IPsec Authentication RSA Private Key - Z
Zeroize SFTP Password	✓	✓	Zeroize SFTP Password	Command	Status output	SFTP Password - Z

2.4.3 Non-Approved Services

The module performs service-by-service switching between FIPS-Approved and non-Approved mode. Table 11 – Non-Approved Services below lists the services available in the non-Approved mode of operation.

Table 11 – Non-Approved Services

Service	Operator		Security Function(s)
	CO	User	
Configure SNMPv2	✓	✓	None
Send/Receive SNMPv2 traps	✓	✓	SNMPv2 KDF (non-compliant)

2.4.4 Authentication

The module does not support authentication mechanisms. The operator implicitly assumes the set of roles consisting of the CO and User when accessing the module.

2.5 Physical Security

The IPsec IPGW is a multiple-chip standalone cryptographic module. The module consists of a hard metal enclosure with production-grade components that include standard passivation techniques.

2.6 Operational Environment

The module does not provide a general-purpose OS to the user. The module has an Intel Xeon-Gold 6230 processor, which runs CentOS 8.2.2004. The module offers no mechanisms for the operator to modify software/firmware components of the operating system, nor does it offer a way to load and execute software or firmware that was not included as part of the module validation. Only the signed image installed on the module can be executed

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 12.

Table 12 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
Firmware Verification Key	2048-bit RSA public key	Generated externally and installed at the factory during staging	Never exits the module	Plaintext in non-volatile memory	N/A	Used in firmware integrity check and firmware load test
SFTP Password	Plaintext string	Installed at the factory during staging	Never exits the module	Obfuscated in non-volatile memory	Zeroize SFTP Password service	Used for SFTP authentication in MGC. MGC downloads files from NMS over SFTP to the IPsec IPGW appliance.
IKE/IPsec Authentication CA Certificate	2048-bit RSA public key	Generated externally and installed during initial configuration	Never exits the module	Plaintext in configuration file in non-volatile memory	Zeroize service	Authentication during IKE/IPsec session negotiation
IKE/IPsec Authentication Certificate	2048-bit RSA public key	Generated externally and installed during initial configuration	Never exits the module	Plaintext in configuration file in non-volatile memory	Zeroize service	Authentication during IKE/IPsec session negotiation
IKE/IPsec Authentication RSA Private Key	2048-bit RSA private key	Generated externally and installed during initial configuration	Never exits the module	Plaintext in configuration file in non-volatile memory	Zeroize service	Authentication during IKE/IPsec session negotiation
DH Public Key (DH public key component)	2048 and 4096-bit DH public key	Internally generated based on SafePrime key generation method	Exits the module in plaintext	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys
DH Secret Key (DH private key component)	2048 and 4096-bit DH private key	Internally generated based on SafePrime key generation method	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Derivation of the IKE/IPsec Session Keys and IKE/IPsec Authentication Keys
IKE Shared Secret	Shared Secret	Derived internally via DH shared secret computation	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Derivation of the IKE Session Key and IKE Authentication Key

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
IKE Session Key	256-bit AES key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Encryption and decryption of IKE session packets
IKE Authentication Key	256-bit HMAC key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Authentication of IPsec session packets
IPSec Shared Secret	Shared Secret	Derived internally via DH shared secret computation	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Derivation of the IPsec Session Key and IPsec Authentication Key
IPsec Session Key	256-bit AES key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Encryption and decryption of IPsec session packets
IPsec Authentication Key	256-bit HMAC key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Zeroize service, Reboot; power cycle; session termination	Authentication of IPsec session packets
DRBG Seed	440-bits random data	Generated internally from entropy source	Never exits the module	Plaintext in volatile memory	Reboot or power cycle	Seed material for Hash DRBG
DRBG Entropy	256-bits random data	Generated internally using nonce along with entropy	Never exits the module	Plaintext in volatile memory	Reboot or power cycle	Entropy material for Hash DRBG
DRBG ‘V’ Value	Internal state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot or power cycle	Used for Hash DRBG
DRBG ‘C’ Value	Internal state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot or power cycle	Used for Hash DRBG

2.8 EMI / EMC

The IPsec IPGW was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed automatically by the module when the module is first powered up and loaded into memory as well as conditionally. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The IPsec IPGW performs the following self-tests at power-up:

- IPsec IPGW Firmware:
  - Firmware integrity Test (2048-bit RSA with SHA-256)
  - AES encrypt and decrypt KAT[29] (CBC-mode)
  - DRBG KAT (NIST SP800-90A Hash DRBG)
  - HMAC KATs using SHA-1 (160-bit) and SHA2 (256-bit)
  - DH Primitive "Z" Computation KATs for 2048-bit and 4096-bit

NOTE: A separate test for SHA-1 and SHA-2 is not needed as these algorithms are tested in the HMAC KATs. A separate test for RSA signature verification is not needed, as this algorithm is tested in the Firmware Integrity Test.

- MGC Firmware:
  - Firmware integrity test (2048-bit RSA with SHA-256)
  - AES encrypt and decrypt KAT[30] (CBC-mode)
  - DRBG KAT (NIST SP800-90A Hash DRBG)
  - HMAC KATs using SHA-1 (160-bit) and SHA-2 (256-bit)
  - RSA sign/verify KAT

NOTE: A separate test for SHA-1 and SHA-2 are not needed as these algorithms are tested in the HMAC KATs.

- Kernel:
  - Hughes IPsec IPGW Kernel Crypto Library 1.0
    - AES encrypt and decrypt KAT (CBC-mode)
    - HMAC KATs using SHA-1 and SHA-256

NOTE: A separate test for SHA-1 and SHA-2 is not needed as these algorithms are tested in the HMAC KATs.

2.9.2 Conditional Self-Tests

The IPsec IPGW performs the following conditional self-tests:

- IPsec IPGW Firmware:

[29] KAT – Known Answer Test
[30] KAT – Known Answer Test

- A vendor defined continuous health test (CHT) on the entropy source (No direct implementation of the RCT or APT are implemented, however the vendor defined health test will reject all samples rejected by the RCT or APT in addition to other samples indicative of a failure mode of the source).

The CHT test is performed over 65536 consecutive samples, which exceed the requirement for 1024

- MGC Firmware:
  - IPGW Firmware Load Test (2048-bit RSA with SHA-256)

The module performs all applicable assurances for its key agreement scheme as specified in section 9 of *NIST SP 800-56Arev3*.

2.9.3 Critical Function Self-Tests

The IPsec IPGW Firmware performs health checks for the DRBG's Generate, Instantiate, and Reseed functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These tests are performed at module power-up.

The MGC Firmware performs health checks for the DRBG's Generate, Instantiate, and Reseed functions as specified in section 11.3 of *NIST SP 800-90Arev1*. These tests are performed at module power-up.

2.9.4 Self-Test Failures

If the firmware integrity test, power-up self-tests, or DRBG health checks fail, the module enters a critical error where all cryptographic functions and data output services are inhibited. A critical error is logged in the /opt/<IPSec IPGW Device ID>/logs/ipgw.log file and sent to the operator. An internal monitoring system checks the log file for errors. When a critical error is detected, the internal monitoring system reboots the module, setting it back to an operational state. If the module cannot be set back to an operational state, then the module is considered to be malfunctioning or compromised, and Hughes Customer Support must be contacted.

If the firmware load test fails, the firmware load process is aborted and no firmware is loaded; however, no module halts or restarts are required to clear the error state. This is a transient error state; once the module sends a status message of the error, then the error state is automatically cleared, and the module returns to a fully operational state.

If any other conditional self-test fails, the module enters a critical error where all cryptographic functions and data output services are inhibited. A critical error is logged in the /opt/<IPGW Device ID>/logs/ipgw.log file and sent to the operator. An internal monitoring system checks the log file for errors. When a critical error is detected, the internal monitoring system reboots the module. Once rebooted, the module performs all power-up self-tests. If completed successfully, the module returns to an operational state where the conditional self-tests can be retried, or a new service performed. If the conditional self-test error persists, then the module is considered to be malfunctioning or compromised, and Hughes Customer Support must be contacted.

The module outputs status on both success and failure of the power-up self-tests. If the self-tests complete successfully, the module sends a "The KAT tests are pass" message to the /opt/<IPGW Device ID>/logs/ipgw.log file. If the self-tests fail, the module sends a "ERROR: Exit the IPGW because KAT Test Failure" message to the /opt/<IPGW Device ID>/logs/ipgw.log file.

2.10 Mitigation of Other Attacks

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

3. Secure Operation

The sections below describe how to place and keep the module in the FIPS-approved mode of operation. **Any operation of the module without following the guidance provided below will result in non-compliant use and is outside the scope of this Security Policy.**

3.1 Initial Setup and Installation

Before the IPsec IPGW is shipped to the customer, it is hot staged by Hughes network engineers. During hot staging, the IPsec IPGW firmware is installed onto the HPE DL360 Gen10 Server. The module is configured, including all settings to operate in a FIPS-Approved mode, and all keys are loaded. The module is field tested to ensure proper operation. After hot staging is complete, the CO shall receive the pre-configured IPsec IPGW server from Hughes via trusted couriers (e.g. United Parcel Service, Federal Express, etc.).

On receipt, the CO must check the package for any irregular tears or openings. If any such damage exists, the CO shall contact Hughes immediately for instructions. The CO shall also retain the packing list, making sure all the items on the list are present.

In order to physically install the module correctly, the CO shall follow the instructions in the *JUPITER Gateway Installation Guide.* The CO must confirm that the IPsec IPGW is operating in a FIPS-Approved mode of operation by opening the Web UI and verifying that “FIPS Mode = Enabled”.

3.2 Crypto Officer Guidance

The CO is responsible for ensuring that the module is operating in its FIPS-Approved mode of operation. When configured according to this Security Policy, the module only runs in a FIPS-Approved mode of operation.

3.2.1 Monitoring Status

The CO shall be responsible for regularly monitoring the module’s status for FIPS-Approved mode of operation. When configured according to the CO guidance in this Security Policy, the module only operates in the FIPS-Approved mode. The CO may view the module’s operational status through the status indicator displayed in the Web UI or by checking the log file, /var/log/mgc.log: FIPS MODE Enable.

3.2.2 Firmware Loading

The module’s firmware can be updated using the external NMS UI. After the module receives a new firmware image to load, the MGC executes the 2048-bit RSA with SHA-256 Firmware Load Test. If the test is passed, the new firmware is loaded, and the module automatically reboots to activate the new firmware. If the test is failed, the new firmware is discarded, and the module returns to normal operation.

Please note that, to maintain the module's validation status, only FIPS-validated firmware shall be loaded. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this Security Policy and will require a separate FIPS 140-2 validation.

3.2.3 Zeroization

To zeroize all plaintext non-ephemeral keys and CSPs (except SFTP Password), the CO must perform the following steps:

1. Open the MGC GUI
2. Navigate to **MGC → IPGW Zeroization**
3. Select the "**CLICK HERE**" link to initiate the zeroization process
4. Once initiated, a popup log, listing the keys and certificates being zeroized, is displayed
5. When the **"Zeroization Done"** status appears in the popup log, then the keys and CSPs are successfully zeroized

To zeroize the SFTP password, the CO must perform the following steps:

1. Open the MGC GUI
2. Navigate to **MGC -> SFTP Zeroization**
3. Select the "**CLICK HERE**" link to initiate the SFTP zeroization process
4. Once initiated, a popup log, listing the files being zeroized, is displayed
5. When the **"SFTP Zeroization Done"** status appears in the popup log, the SFTP password has been zeroized.

Once invoked, the effect of the zeroization process is immediate and will not allow enough time to compromise any stored plaintext keys or CSPs.

3.3 User Guidance

While the CO is responsible for ensuring that the module's physical security mechanisms are in place and that the module is running in a FIPS-Approved mode of operation, Users should also monitor appliance status. Any changes in the status of the module should immediately be reported to the CO.

3.4 Additional Guidance and Usage Policies

This section notes additional guidance and policies that must be followed by module operators.

- To execute the module's power-up self-tests on-demand, the module's host device can be rebooted or power-cycled.

4. Appendix

4.1 Acronyms

Table 13 provides definitions for the acronyms used in this document.

Table 13 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CKG	Cryptographic Key Generation
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CSP	Critical Security Parameter
CST	Conditional Self-Test
CTR	Counter
CVL	Component Validation List
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
GHz	Gigahertz
GW	Gateway
HMAC	(keyed-) Hash Message Authentication Code
IKE	Internet Key Exchange
iLO	Internet Lights Out
IP	Internet Protocol

Acronym	Definition
IPsec	Internet Protocol Security
KAS	Key Agreement Scheme
KAS-SSC	Key Agreement Scheme – Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
KPG	Key Pair Generation
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest v5
MFS	Management File Server
MGC	Management Gateway Client
N/A	Not Applicable
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NMS	Network Management Server
OS	Operating System
PCIe	PCI express
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSK	Pre-Shared Key
PUB	Publication
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SP	Special Publication
UI	User Interface
UID	Unit Identification
U.S.	United States
USB	Universal Serial Bus

Acronym	Definition
VGA	Video Graphics Array
VoIP	Voice Over Internet Protocol
VSAT	Very Small Aperture Terminal

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com