Information Assurance Specialists, Inc.

IAS Router

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Version: 2

Date: June 21, 2016

Table of Contents

1 Introduction 5

Hardware and Physical Cryptographic Boundary 6
1.1 Modes of Operation 11

2 Cryptographic Functionality 12

2.1 Critical Security Parameters 16
2.2 Public Keys 17

3 Roles, Authentication and Services 17

3.1 Assumption of Roles 17
3.2 Authentication Methods 18
3.2.1 Password-based Authentication 18
3.2.2 IPSec Authentication 18
3.3 Services 19

4 Self-tests 22

5 Physical Security Policy 23

5.1 IAS STEW 23
5.2 KG-RU 25
5.3 IAS Router Micro 28

6 Operational Environment 30

7 Mitigation of Other Attacks Policy 30

8 Security Rules and Guidance 31

9 References and Definitions 32

List of Tables

Table 1 – IAS Router Configurations 5
Table 2 – Security Level of Security Requirements 5
Table 3 – IAS Router Micro Port and Interface Identification 7
Table 4 – IAS STEW Ports and Interfaces 9
Table 5 – IAS KG-RU Ports and Interfaces 11
Table 6 – Approved and CAVP Validated Cryptographic Functions 12
Table 7 – Approved Cryptographic Functions Tested with Vendor Affirmation 13
Table 8 – Non-Approved but Allowed Cryptographic Functions 13
Table 9 – Protocols Allowed in FIPS Mode 14
Table 10 – Critical Security Parameters (CSPs) 16
Table 11 – Public Keys 17
Table 12 – Roles Description 17
Table 13 – Authentication Description 19
Table 14 – Authenticated Services 19
Table 15 – Unauthenticated Services 19
Table 16 – CSP Access Rights within Services 20
Table 17 – Power Up Self-tests 22
Table 18 – Conditional Self-tests 22
Table 19 – Physical Security Inspection Guidelines 30
Table 20 – References 32
Table 21 – Acronyms and Definitions 32

List of Figures

Figure 1: IAS Router Micro Port and Interface Identification 6
Figure 2: IAS STEW Ports and Interfaces 8
Figure 3: IAS KG-RU Rear Panel Ports and Interfaces 10
Figure 4: IAS KG-RU Front Panel Ports and Interfaces 10
Figure 5: IAS STEW Top View 23
Figure 6: IAS STEW Right Side 24
Figure 7: IAS STEW Left Side 24
Figure 8: IAS STEW Bottom 25
Figure 9: IAS KG-RU Top Image 26
Figure 10: IAS KG-RU Top Corner 26
Figure 11: IAS KG-RU Side View 27

Figure 12: IAS KG-RU bottom 27
Figure 13: IAS Router Micro Bottom View 28
Figure 14: IAS Router Micro Right Side 29
Figure 15: IAS Router Micro Left Side 29
Figure 16: Tamper Evidence 30

1 Introduction

This document defines the Security Policy for the Information Assurance Specialists, Inc. IAS Router module. The IAS Router is an IPSec VPN gateway. The IAS Router meets FIPS 140-2 overall Level 2 requirements.

Table 1 – IAS Router Configurations

	Module	HW P/N and Version	FW Version
1	IAS Router	IAS STEW Rev 1.0	50e8756 – 2015-11-24
2	IAS Router	IAS KG-RU Rev 1.0	50e8756 – 2015-11-24
3	IAS Router	IAS Router Micro Rev 1.0	50e8756 – 2015-11-24

The IAS Router is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated cryptographic implementations in a VPN gateway. The IAS Router is a Multi-Chip Standalone embodiment; the cryptographic boundary is defined as the device enclosure.

The IAS STEW Rev 1.0 and IAS KG-RU Rev 1.0 exclude the Cisco ESR5915 component from the requirements of FIPS 140-2. The Cisco ESR5915 has been FIPS 140-2 Validated (Cert. #2241); however, the KG-RU treats all data to/from the Cisco ESR5915 component as plaintext. The Cisco ESR5915 component cannot affect the security of the Module.

The IAS Router Micro Rev 1.0 excludes the Unicom 4GT24-57INL component from the requirements of FIPS 140-2. This is a passive component and has no security functionality.

The FIPS 140-2 security levels for the IAS Router are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Hardware and Physical Cryptographic Boundary

The physical form of the IAS Router is depicted in Section 5; the physical cryptographic boundary is the enclosure. The IAS Router provides network connectivity over its Ethernet, Wi-Fi, and USB interfaces.

Figure 1 through Figure 4 depict the ports and interfaces provided by the IAS Router. The Network interface consists of the FIPS 140-2 Data Input, Data Output, Control Input, and Status Output interfaces.

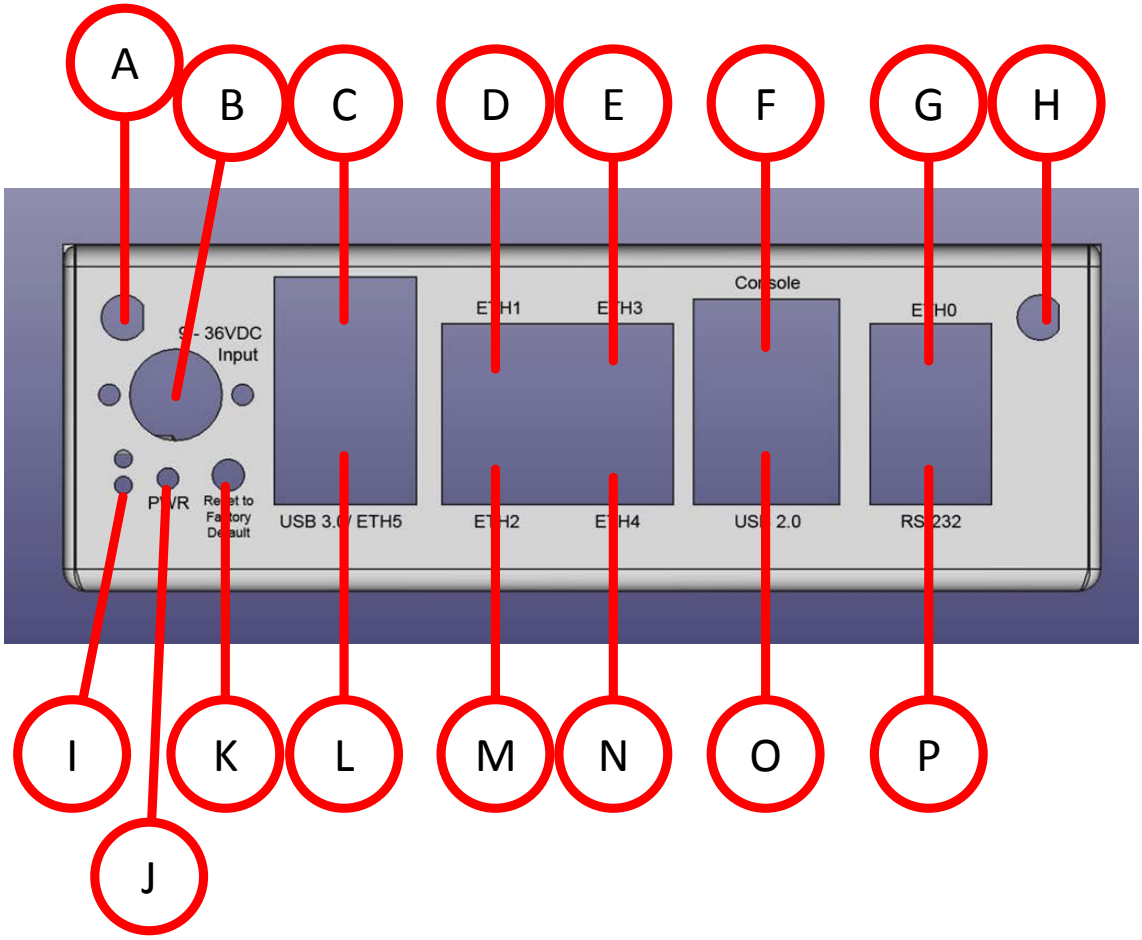


Figure 1: IAS Router Micro Port and Interface Identification

Table 3: IAS Router Micro Port and Interface Identification

Ref	Port Type	Subsystem	Port Identifier	Logical Interface
A	RP-SMA Wi-Fi Antenna	IAS Router		Network
B	Power In	Power	9-36VDC Input	Power (input)
C	Gigabit Ethernet Port	IAS Router	ETH5	Network
D	Gigabit Ethernet Port	IAS Router	ETH1	Network
E	Gigabit Ethernet Port	IAS Router	ETH3	Network
F	Console Port	IAS Router	CONSOLE	Control (input) Status (output)
G	Fast Ethernet Port	IAS Router	ETH0	Network
H	RP-SMA Wi-Fi Antenna	IAS Router		Network
I	Status (top) and Power (bottom) LED	IAS Router		Status
J	Power Button	IAS Router	PWR	Control (input)
K	Reset to Factory Defaults Button	IAS Router	Reset to Factory Default	Control (input)
L	USB 3.0 ports	IAS Router	USB3.0	Network
M	Gigabit Ethernet Port	IAS Router	ETH2	Network
N	Gigabit Ethernet Port with Power over Ethernet 802.3af	IAS Router	ETH4	Network
O	USB 2.0 Ports	IAS Router	USB 2.0	Network
P	Auxiliary Serial Port	IAS Router	SERIAL	Control (output)
Q	Power Out (on rear, not shown)	Power		Power (output)

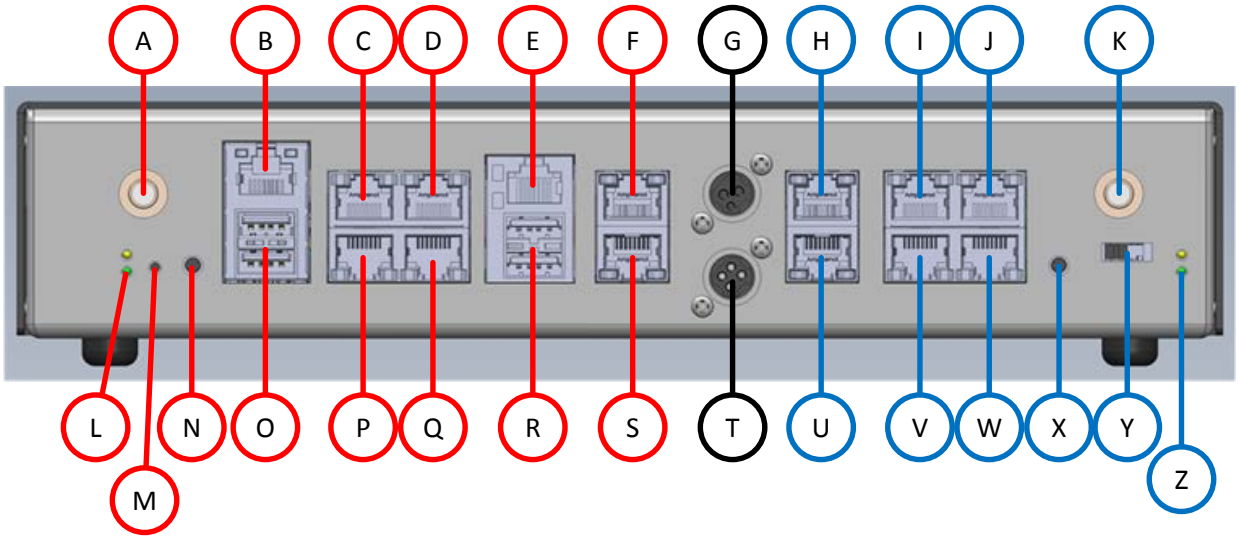


Figure 2: IAS STEW Ports and Interfaces

Table 4: IAS STEW Ports and Interfaces

Ref	Port Type	Subsystem	Port Identifier	Logical Interface
A	RP-SMA Wi-Fi Antenna	IAS Router		Network
B	Gigabit Ethernet Port	IAS Router	ETH5	Network
C	Gigabit Ethernet Port	IAS Router	ETH1	Network
D	Gigabit Ethernet Port	IAS Router	ETH3	Network
E	Console Port	IAS Router	CONSOLE	Control (input) Status (output)
F	Fast Ethernet Port	IAS Router	ETH0	Network
G	Power Out (optional)	Power		Power (output)
H	Fast Ethernet Port	Cisco	FE0/0	Network
I	Fast Ethernet Port	Cisco	FE0/1	Network
J	Fast Ethernet Port	Cisco	FE0/3	Network
K	RP-SMA Wi-Fi Antenna	Cisco		Network
L	Status (top) and Power (bottom) LED	IAS Router		Status
M	Power Button	IAS Router		Control (input)
N	Reset to Factory Defaults Button	IAS Router		Control (input)
O	USB 3.0 ports	IAS Router		Network
P	Gigabit Ethernet Port	IAS Router	ETH2	Network
Q	Gigabit Ethernet Port with Power over Ethernet 802.3af	IAS Router	ETH4	Network
R	USB 2.0 Ports	IAS Router		Network
S	Auxiliary Serial Port	IAS Router	SERIAL	Control (output)
T	Power In	Power		Power (input)
U	Console Port	Cisco	CONSOLE	Control (input) Status (output)
V	Fast Ethernet Port	Cisco	FE0/2	Network
W	Fast Ethernet Port with Power over Ethernet 802.3af	Cisco	FE0/4	Network
X	Reset to Factory Defaults Button	Cisco		Control (input)
Y	Power Switch	Cisco		Control (input)
Z	Status (top) and Power (bottom) LEDs	Cisco		Status (output)

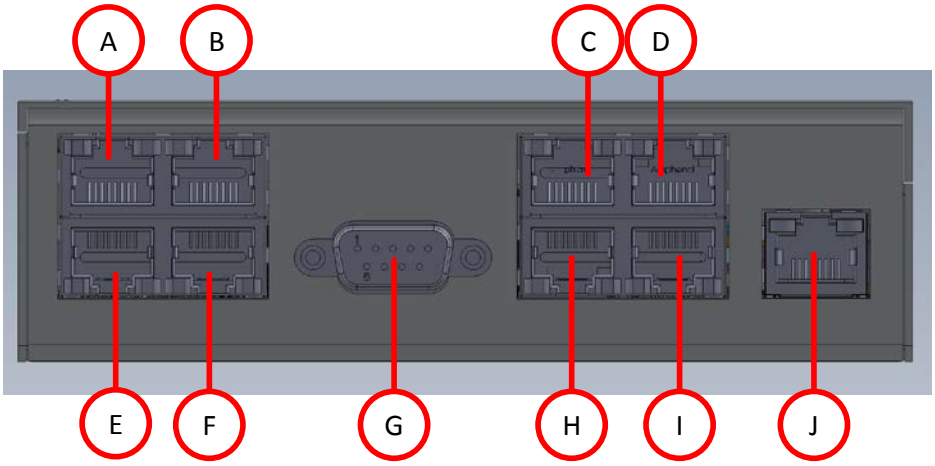


Figure 3: IAS KG-RU Rear Panel Ports and Interfaces

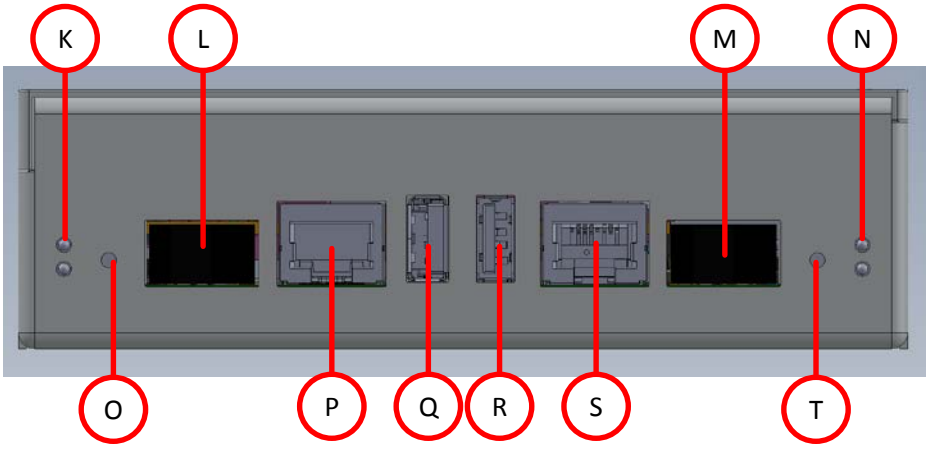


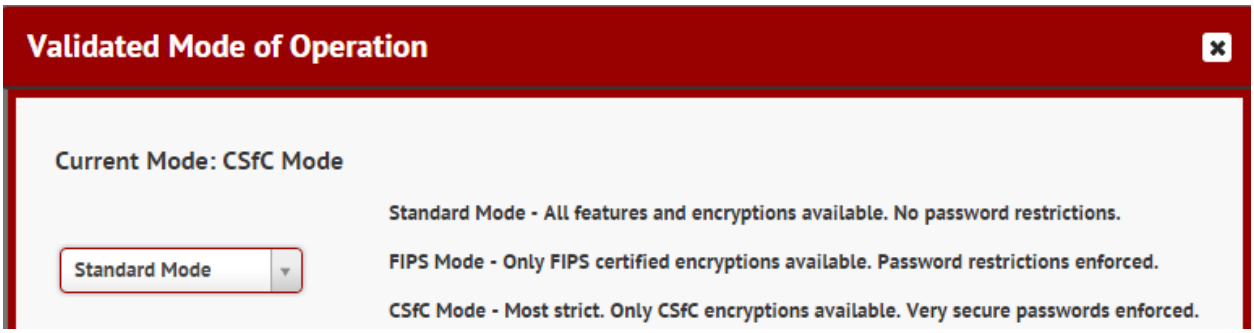
Figure 4: IAS KG-RU Front Panel Ports and Interfaces

Table 5: IAS KG-RU Ports and Interfaces

Ref	Port Type	Subsystem	Port Identifier	Logical Interface
A	Fast Ethernet Port	Cisco	FE0/1	Network
B	Fast Ethernet Port	Cisco	FE0/3	Network
C	Gigabit Ethernet Port	Cisco	ETH2	Network
D	Gigabit Ethernet Port	Cisco	ETH3	Network
E	Fast Ethernet Port	Cisco	FE0/2	Network
F	Fast Ethernet Port with Power over Ethernet 802.3af	Cisco	FE0/4	Network
G	Power In	Power	9-36VDC Input	Power (input)
H	Gigabit Ethernet Port	IAS Router	ETH4	Network
I	Gigabit Ethernet Port	IAS Router	ETH5	Network
J	Gigabit Ethernet Port	IAS Router	ETH1	Network
K	Status (top) and Power (bottom) LEDs	IAS Router	STATUS, PWR	Status (output)
L	Power Switch	IAS Router	PWR	Control (input)
M	Power Switch	Cisco	PWR	Control (input)
N	Status (top) and Power (bottom) LEDs	Cisco	STATUS, PWR	Status (output)
O	Reset to Factory Defaults Button	IAS Router	RESET	Control (input)
P	Console Port	IAS Router	CONSOLE	Control (input) Status (output)
Q	USB 3.0 ports	IAS Router	USB	Network
R	USB 2.0 Ports	IAS Router	USB	Network
S	Console Port	Cisco	CONSOLE	Control (input) Status (output)
T	Reset to Factory Defaults Button	Cisco	RESET	Control (input)

1.1 Modes of Operation

The Module operates in three (3) distinct modes of operation: Standard Mode, FIPS Mode, and CSfC Mode. The Standard Mode is a non-FIPS mode of operation. The FIPS Mode and CSfC Mode are FIPS Approved modes of operation. The non-Approved mode of operation, Standard Mode, supports the identical services as FIPS Mode and CSfC Mode; however, it supports the non-Approved algorithms listed in Table 9. To verify that a module is in the Approved mode of operation, authenticate to the web management page and check the mode indicator on the System Configuration page as depicted below.



2 Cryptographic Functionality

The IAS Router implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the table below.

Table 6 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
Triple-DES	[FIPS 46-3, SP 800-67] Functions: Encryption, Decryption Modes: DES-EDE3-CBC Key sizes: 168 bits (DES-EDE3)	1935
AES	[FIPS 197, SP 800-38A, SP800-38D] Functions: Encryption, Decryption Modes: CBC, CTR, GCM Key sizes: 128, 256 bits	3430
DRBG	[SP 800-90A] Functions: AES 256 CTR DRBG Security Strengths: 256 bits	782
ECDSA	[FIPS 186-4] Functions: Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation Curves/Key sizes: P-256, P-384, P-521	663
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA: 1, 256, 384, 512	2182

Algorithm	Description	Cert #
KDF, Existing Application-Specific	[SP 800-135] Functions: IKE v1 KDF, IKEv2 KDF	493 (CVL)
KDF, Existing Application-Specific	[SP 800-135] Functions: TLS v1.0/1.1 KDF, TLS 1.2 KDF	523 (CVL)
RSA	[FIPS 186-4, PKCS #1 v2.1 (PKCS1.5)] Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	1756
SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512	2830

Table 7 – Approved Cryptographic Functions Tested with Vendor Affirmation

Algorithm	Description	IG Ref.
Key Transport Using RSA	[SP 800-56B] Key sizes: 2048, 3072, 4096, 6144, 8192 bits	Vendor Affirmed IG D.4

Table 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
Non-SP 800-56A Compliant DH	[IG D.8] Diffie-Hellman (key agreement; key establishment methodology provides 112, 128, or 192 bits of encryption strength)
Non-SP 800-56A Compliant ECDH	[IG D.8] EC Diffie-Hellman (key agreement; key establishment methodology provides 128, 192, or 256 bits of encryption strength)
NDRNG	[Annex C] Hardware Non-Deterministic RNG; minimum of 256 bits per access. The NDRNG output is used to seed the FIPS Approved AES 256 CTR DRBG.
MD5	[IG G.13] TLSv1.0 and TLSv1.1 KDF. No security is provided by this algorithm.

Table 9 – Protocols Allowed in FIPS Mode

Protocol/Operation	Algorithm	Standard Mode	FIPS Mode	CSFC Mode
		1	2	3
IKE				
Encryption	3des	x	X	
	AES128CBC	x	X	x
	AES256CBC	x	x	x
Integrity	md5	x		
	Sha	x		
	sha256	x	x	x
	sha384	x	x	x
	sha512	x	x	
Key Exchange	dh1 - modp768	x		
	dh2 – modp1024	x		
	dh5 – modp1536	x		
	dh14 – modp2048	x	x	x
	dh15 – modp3072	x	x	
	dh16 – modp4096	x	x	
	dh17 – modp6144	x	x	
	dh18 – modp8192	x	x	
	dh19 – ecp256	x	x	x
	dh20 – ecp384	x	x	x
	dh21 – ecp521	x	x	x
PRF	matches selected IKE integrity algo			
ESP				
Encryption	3des	x	x	
	AES128CBC	x	x	x
	AES256CBC	x	x	x
	AES128CTR	x	x	
	AES256CTR	x	x	
	AES128GCM16	x		x
	AES256GCM16	x		x
Integrity	md5	x		
	Sha	x		
	sha256	x	x	x
	sha384	x	x	x
	sha512	x	x	x
PFS Key Exchange	No PFS	x		
	dh1 - modp768	x		
	dh2 – modp1024	x		
	dh5 – modp1536	x		
	dh14 – modp2048	x	x	x

Protocol/Operation	Algorithm	Standard Mode	FIPS Mode	CSFC Mode
		1	2	3
	dh15 – modp3072	x	x	
	dh16 – modp4096	x	x	
	dh17 – modp6144	x	x	
	dh18 – modp8192	x	x	
	dh19 – ecp256	x	x	x
	dh20 – ecp384	x	x	x
	dh21 – ecp521	x	x	x
IKE Authentication				
PSK	adhere to password complexity rules	x	x	x
Certificate signature algorithms	rsa_with_sha1	x		
	rsa_with_sha256	x	x	
	rsa_with_sha384	x	x	
	rsa_with_sha512	x	x	
	ecdsa_with_sha1	x		
	ecdsa_with_sha256	x	x	x
	ecdsa_with_sha384	x	x	x
	ecdsa_with_sha512	x	x	
Certificate private key types	RSA 1024	x		
	RSA 2048	x	x	
	RSA 4096	x	x	
	EC on p256	x	x	X
	EC on p384	x	x	X

Protocol/ Operation	Algorithm (RFC)	Standard Mode	FIPS Mode	CSFC Mode
TLS 1.0/1.1/1.2 Ciphers				
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	x	x	x
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	x	x	x
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	x	x	x
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	x	x	x
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	x	x	x
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	x	x	x
	TLS_RSA_WITH_AES_256_CBC_SHA256	x	x	x
	TLS_RSA_WITH_AES_128_CBC_SHA256	x	x	x

Protocol/ Operation	Algorithm (RFC)	Standard Mode	FIPS Mode	CSFC Mode
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	x	x	x
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	x	x	x
	TLS_RSA_WITH_AES_256_CBC_SHA	x	x	x
	TLS_RSA_WITH_AES_128_CBC_SHA	x	x	x

These protocols have not been reviewed or tested by the CAVP or CMVP.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- MD5 (outside of the TLS KDF)
- Diffie-Hellman (modp < 2048, provides less than 112 bits of encryption strength)
- RSA (any size) with SHA-1
- RSA 1024

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in Section 4.

Table 10 – Critical Security Parameters (CSPs)

Number	CSP	Description / Usage
1	TLS DH/ECDH Private Key	Used to agree upon a secret that is used as input to the pre_master_secret
2	RSA TLS_pre_master_secret	TLS secret used to derive the master_secret
3	DH/ECDH TLS_pre_master_secret	TLS secret used to derive the master_secret
4	TLS_master_secret	TLS secret used to derive the session_key
5	TLS_session_key	TLS session secret key
6	TLS_PKI_private	Certificate private key used to negotiate session keys for TLS sessions
7	IKE DH/ECDH Private Key	Used to agree upon a secret that is used as input to derive the IKE Session key
8	IPSec_PSK	Shared secret value used in IKE and ESP session keys negotiation
9	IPSec_PKI_private	Certificate private key used to negotiate ESP and IKE session keys
10	IPSec_IKE_key	IKE session secret key
11	IPSec_ESP_key	ESP session secret key

Number	CSP	Description / Usage
12	Administrator PW	Used to authenticate administrative users

2.2 Public Keys

Table 11 – Public Keys

Key	Description / Usage
TLS DH/ECDH Public Key	Used to agree upon a secret that is used as input to the pre_master_secret
TLS_PKI_public	Certificate public key used to negotiate session keys for TLS sessions
IKE DH/ECDH Public Key	Used to agree upon a secret that is used as input to derive the IKE session key
IPSec_PKI_public	Certificate public key used to negotiate ESP and IKE session keys
IPSec_PKI_CA_public	CA certificates

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports two (2) distinct operator roles, User and Cryptographic Officer (CO). The cryptographic module enforces the separation of roles by requiring the CO to authenticate to gain access to CO operations.

Table 12 lists all operator roles supported by the IAS Router. The IAS Router supports concurrent operators. Operators can login via the web management interface. Authenticated operator sessions can be manually terminated using the logout feature or if the device is reboot all authenticated sessions are automatically terminated. User authentication passwords are protected within the device via a hash mechanism, are masked while the user is entering the value, and are protected in transmission by TLS.

The IAS Router does not support a maintenance role.

Table 12 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – The Crypto Officer configures the services provided by the module and is authenticated by password-based authentication	Identity based	Username and password
User	User – The User is a network entity that can establish an IPSec VPN	Role based	IKE PSK, RSA signature, ECDSA signature

3.2 Authentication Methods

All authentication data is protected from modification and substitution within the IAS Router by restricting physical access to the internal storage media. When performing remote administration authentication data is protected in flight through the HTTPS/SSL/TLS encrypted management web page. Authentication data is protected during entry by masking all authentication data entry fields.

3.2.1 Password-based Authentication

Passwords are required to have a minimum length of 8 characters in FIPS mode. Of the 8 characters there must be a capital letter, a lowercase letter, a number, and a special character. The module supports the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Characters can repeat within the password. Therefore the possibility of randomly guessing the correct characters of a minimum length password (independent of sequence) is 1 in 26^2 * 10 * 10 * 72^4 = 1,816,672,665,600.

On the GUI, Authentication attempts are limited to 1-19 successive incorrect attempts results in a 1-19 minute authentication attempt lockout. Therefore, the maximum number of attempts in a 1 minute window is 19 and the probability of successfully guessing the password in a One (1) minute period of time is approximately 1 in 85,425,052,631.

On the rescue terminal, successive authentication attempts are limited to every 4 seconds. Therefore, a maximum of 15 authentication attempts can be made within a minute and the probability of guessing the password within a one (1) minute period of time is approximately 1 in 108,205,066,667.

3.2.2 IPSec Authentication

The module supports RSA-based, ECDSA-based and Pre Shared Key authentication for IPSec. On IPSec, authentication attempts occur within a session. Each IPSec authentication session remains active until it either succeeds or times out after 30 seconds. There are several limits to the number of simultaneous authentication attempts in place. Simultaneous authentication attempts from a peer (defined as an IP source address) are limited to 5. System wide simultaneous authentication attempts are limited to 50. Therefore, the theoretical maximum of authentication attempts in a 1 minute window is 100 and the probability of successfully guessing the worst case IPsec authentication method (Pre-Shared Key) is 100 in 1,623,076,000,000 or 1 in 16,230,760,000.

3.2.2.1 RSA-based Authentication

When using RSA based authentication the smallest modulus allowed is 2048, which has 112-bits of strength. Therefore, the probability of successfully randomly guessing the authentication value is 1 in 2^{112}.

3.2.2.2 ECDSA-based Authentication

When using ECDSA based authentication the weakest curve is P-256 which has 128-bits of strength. Therefore, the probability of successfully randomly guessing the authentication value is 1 in 2^{128}.

3.2.2.3 Pre Shared Key (PSK)-based Authentication

When using PSK based authentication the minimum PSK length is eight (8) characters. The same complexity rules apply as the password-based authentication mechanism.

Table 13 – Authentication Description

Authentication Method	Probability of false acceptance (1.0×10^{-6} required)
Password Auth	$1 / 26^2 * 10^5 * 8 = 5.4 \times 10^{-8}$
PSK Auth	$1 / 26^2 * 10^5 * 8 = 5.4 \times 10^{-8}$
RSA Auth	$1 / 2^{112}$
ECDSA Auth	$1 / 2^{128}$

3.3 Services

All services implemented by the Module are listed in the tables below.

Table 14 – Authenticated Services

Service	Role	Description
Reset to Defaults / Zeroize	CO	Destroys all CSPs
Configure the Router	CO	Define networks/interfaces, firewall behavior, routing, user accounts, user permissions, set the time, enable/disable protocols, etc.
Configure VPN	CO	Manage authentication credentials, IPSec security policies, and IPSec security associations
Show status	CO	View network and interface statistics, active IPSec sessions, and other system status items
Establish/Maintain IPSec VPN	User	Authenticate, establish, maintain, and terminate an IPSec VPN (phase 1 and 2, IKE and CHILD) with another network entity

The Authenticated Services require an administrator or peering IPSec router to authenticate using one if the methods outlined in Section 3.2 prior to accessing the service.

Table 15 – Unauthenticated Services

Service	Description
Route Traffic	Provides processing for user traffic
Module Reset (Self-test)	Reset the IAS Router and invoke a self-test
LED Status	View VPN status LED and power status LED

The Unauthenticated Services are provided for users and administrators.

Table 16 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The Module generates the CSP.
- R = Read: The Module reads the CSP. The read access is typically performed before the Module uses the CSP.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module, when the Module generates a CSP, or when the Module overwrites an existing CSP.
- Z = Zeroize: The Module zeroizes the CSP.

Table 16 – CSP Access Rights within Services

Service	CSPs (as identified in Table 10)
Reset to Defaults / Zeroize	Z – 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12
Configure the Router	G – 3, 4, 5, 6 R – 1, 2, 3, 4, 5, 6, 8, 12 E – 1, 2, 3, 4, 5, 6, 12 W – 6, 8, 9, 12 Z – 2, 3, 4, 5, 6, 8, 9, 12
Configure VPN	G – 9 R – 8, 9 E – 9 W – 8, 9 Z – 8, 9
Show status	–N/A

Service	CSPs (as identified in Table 10)
Establish/Maintain IPSec VPN	G – 7 R – 7, 8, 9, 10, 11 E – 7, 8, 9, 10, 11 W – 7, 10, 11 Z – 7, 10, 11
Route Traffic	G – R – 11 E – 11 W – Z –
Module Reset (Self-test)	G – R – E – W – Z – 1, 2, 3, 4, 5, 7, 10, 11
LED Status	N/A

4 Self-tests

Each time the Module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self-tests are available on demand by power cycling the Module.

On power up or reset, the Module performs the self-tests described in Table 17 below. All KATs must be completed successfully prior to any other use of cryptography by the Module. If the module successfully completes self-tests, it creates a syslog entry indicating successful completion of the self-tests. If one of the KATs fails, the Module enters the Critical Error state, which then causes the Module to reboot.

Table 17 – Power Up Self-tests

Test Target	Description
Firmware Integrity	ECDSA P-256 signature check of a SHA256 message digest is performed on each executable file, the kernel, all kernel modules, and all interpreted php code resident in the image.
AES	KATs: Encryption, Decryption Modes: ECB Key sizes: 128 bits
DRBG	KATs: CTR DRBG Security Strengths: 256 bits
ECDSA	PCT: Signature Generation, Signature Verification Curves/Key sizes: P-256
RSA	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
SHA	KATs: SHA-1, SHA-256, SHA-384, SHA-512
HMAC	KATs: HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512
TDES	KATs: Encryption, Decryption Modes: TECB, Key sizes: 3-key
Key Transport Using RSA	KATs: SP 800-56B specific KATs per IG D.4 Key sizes: 2048 bits

Table 18 – Conditional Self-tests

Test Target	Description
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
ECDSA	ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation.
RSA	RSA Pairwise Consistency Test performed on every RSA key pair generation.

Test Target	Description
Firmware Load	ECDSA P-256 signature check of a SHA256 message digest is performed when firmware is loaded.
DRBG Health Checks	Performed conditionally per SP 800-90A Section 11.3. Required per IG C.1.
Bypass Test	SHA256 checksum validated whenever the bypass configuration (firewall) is altered.

5 Physical Security Policy

Tamper seals are applied during the manufacturing process. A subsection is used for each model of the IAS Router covered under this validation.

5.1 IAS STEW

The IAS STEW is housed in an industrial quality enclosure using production grade components and materials.

The IAS STEW utilizes tamper evident seals to ensure physical security of the Module's internal components. The STEW enclosure has 5 pieces and the application and location of the six tamper evident seals ensures that the 5 pieces remain intact as a complete enclosure and none of the pieces can be surreptitious opened or removed.

Ideally, tamper evident measures should be inspected whenever physical access control of the Module has been lost or interrupted. Devices under kept under physical access control should be inspected monthly.

Figure 5: IAS STEW Top View

Figure 6: IAS STEW Right Side

Figure 7: IAS STEW Left Side

Figure 8: IAS STEW Bottom

5.2 KG-RU

The KG-RU utilizes tamper evident seals to ensure physical security of the Module's internal components. The KG-RU enclosure has three (3) pieces and the application and location of the three (3) tamper evident seals ensures that the three (3) pieces remain intact as a complete enclosure and none of the pieces can be surreptitious opened or removed.

Ideally, tamper evident measures should be inspected whenever physical access control of the Module has been lost or interrupted. Devices kept under physical access control should be inspected monthly.

Figure 9: IAS KG-RU Top Image

Figure 10: IAS KG-RU Top Corner

Figure 11: IAS KG-RU Side View

Figure 12: IAS KG-RU bottom

5.3 IAS Router Micro

The IAS Router Micro utilizes tamper evident seals to ensure physical security of the Module's internal components. The IAS Router Micro enclosure has four (4) pieces and the application and location of the three tamper evident seals ensures that the four (4) pieces remain intact as a complete enclosure and none of the pieces can be surreptitious opened or removed.

Ideally, tamper evident measures should be inspected whenever physical access control of the Module has been lost or interrupted. Devices under kept under physical access control should be inspected monthly.

Figure 13: IAS Router Micro Bottom View

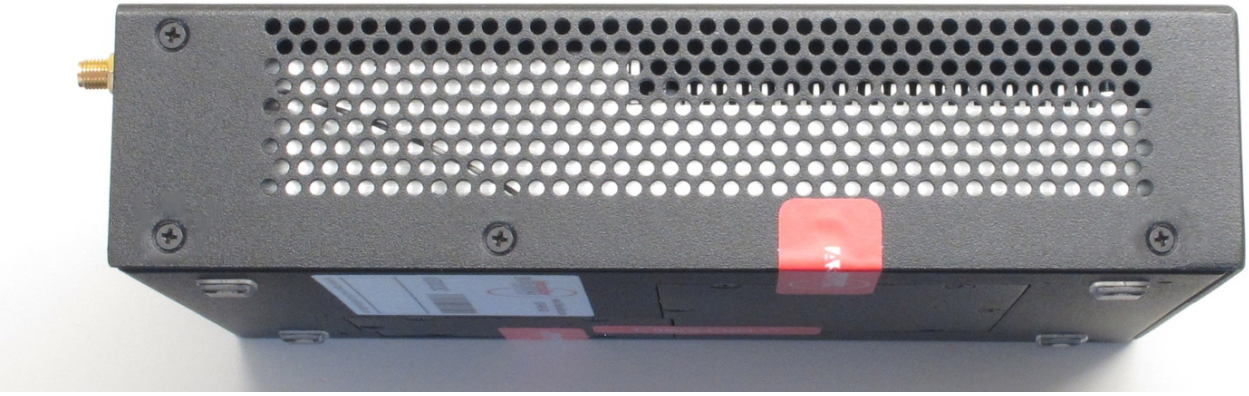


Figure 14: IAS Router Micro Right Side

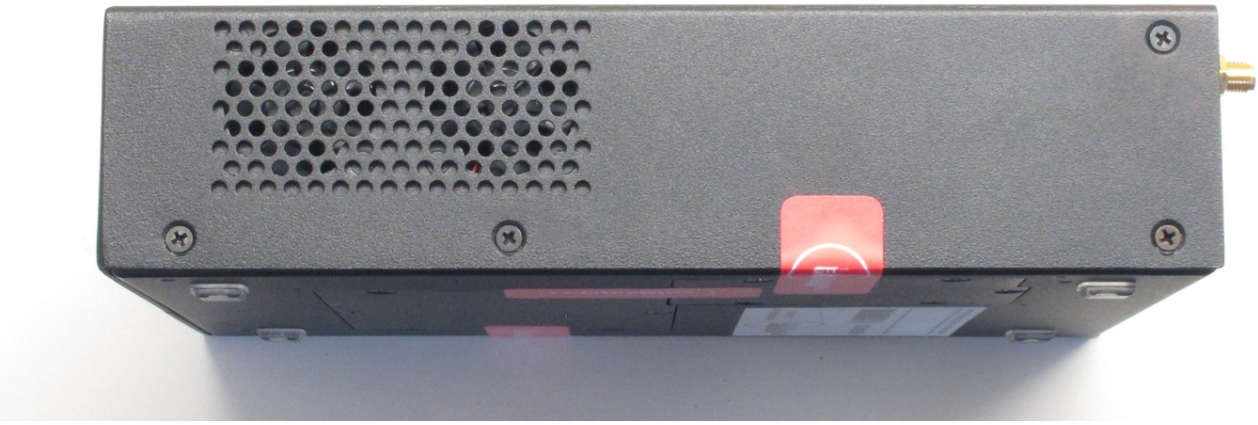


Figure 15: IAS Router Micro Left Side

Table 19 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evident seals	Monthly	Verify that all of the tamper seals are present and in the correct locations as depicted above. Inspect each seal to verify that the word "VOID" does not appear (even faintly). See Figure 16. In the event tamper seals indicate "VOID" (even faintly), the device should be removed from use and returned to IAS for inspection and application of new tamper seals.

Figure 16: Tamper Evidence

6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware update service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

This module does not implement mitigation for any other attacks.

8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The Module provides two (2) distinct operator roles: User and Cryptographic Officer.
2. The Module clears previous authentications on power cycle.
3. The operator can command the module to perform the power up self-tests by cycling power or resetting the Module.
4. Power up self-tests do not require any operator action.
5. Data output is inhibited during key generation, self-tests, zeroization, and error states.
6. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The Module does not support a maintenance interface or role.
8. The Module does not output intermediate key values.
9. The Module performs a bypass test when the mechanism governing bypass is modified.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 20 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[IG]	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, December 28, 2015

Table 21 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IPsec	Internet Protocol Security
NDRNG	Non-Deterministic Random Number Generator
PSK	Pre-Shared Key
RSA	Rivest Shamir Adleman (public-key cryptosystem)
SHA	Secure Hash Algorithms
TLS	Transport Layer Security
VPN	Virtual Private Network