InZero Security Platform

Targeted protection of critical data

FIPS 140-2 SECURITY POLICY FOR:

INZERO GATEWAY

MODULE VERSION: XB2CUSB3.1

INZERO SYSTEMS

Firmware Version 2.80.0.38
Document Version: 2.80.0.n

Table of Contents

1 INTRODUCTION 1

1.1 Purpose 1

1.2 Supporting Documentation 1

2 MODULE SPECIFICATION..2

2.1 InZero Security Platform Architecture..2

2.2 Module Overview 2

2.3 Security Requirements..4

2.4 Roles 4

2.4.1 Authentication 5

2.5 Services 6

2.6 Cryptographic Boundaries 8

2.7 Ports and Interfaces..8

2.8 Self-Tests..10

2.9 Physical Security 12

2.10 Mitigation of Other Attacks..12

3 CRYPTOGRAPHIC KEY MANAGEMENT 13

3.1 Algorithms..13

3.2 Key Generation..14

3.3 Key Storage 14

3.4 Key/CSP Access, Protection and Zeroization..15

4 SECURE OPERATION 17

4.1 Module Initialization (CO) 17
4.1.1 Installing the Module 17
4.1.2 Reset Module to Factory Defaults 17
4.1.3 Generate Configuration Key....... 17
4.1.4 Configure Module for Domain Management 17
4.1.5 Generate Network Key (Optional) 18
4.1.6 Verify Firmware Version and FIPS Fingerprint 18
4.1.7 Configuration Changes....... 18
4.1.8 Change CO Password 18

4.2 Managing External Keys (CO)....... 19

4.3 Module Configuration (CO) 19

4.4 Configuring FIPS Mode VPNs (Network Administrator)....... 19

4.5 Zeroizing the Module (CO)....... 19

4.6 Diagnostics (All Operators)....... 20

Table of Figures

Figure 1 - InZero Security Platform 2
Figure 2 – Module Diagram....... 3
Figure 3 - Cryptographic Boundary 8
Figure 4 - Physical ports 9
Figure 5 - Placement of Right-side Seals....... 12
Figure 6 - Placement of Left-side Seals and Shield 12

Table of Tables

Table 1 - Validation Level by Section....... 4
Table 2 - Roles and Required Identification and Authentication 5
Table 3 - Strength of Authentication Mechanisms....... 5
Table 4 - Services Mapped to Roles 6
Table 5 - Ports and Interfaces....... 10
Table 6 - Power-up Self-tests....... 11
Table 7 - Conditional Self-tests....... 11
Table 8 - Inspection of Physical Security Mechanisms....... 12
Table 9 - Approved Algorithms....... 13
Table 10 - Keys and CSPs 15

1 Introduction

This document describes the non-proprietary security policy for the InZero® Gateway XB2CUSB3.1 Series Cryptographic Module, subsequently referred to as *FIPS module*, *Gateway module, module*, or *Gateway*.

InZero also sells a standard (not FIPS capable) InZero Gateway XB2CUSB3.1 device with different firmware and a similar enclosure. The FIPS module can be identified by the firmware version and presence of four tamper-evident seals and an opacity shield covering the air vents. The rest of this document pertains only to the FIPS module.

1.1 Purpose

The Gateway is a candidate for validation as a Level 2 multi-chip standalone cryptographic module. The Federal Information Processing Standards (FIPS) Publication 140-2, *Security Requirements for Cryptographic Modules,* establishes U.S. requirements for cryptographic modules. This document describes how the Gateway meets these requirements and includes instructions for configuring the Gateway module to operate in a mode ("FIPS mode") consistent with these requirements.

This *Security Policy* document will be available online at the National Institute of Standards and Technology website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) for analysis by potential customers. See InZero's website (http://www.inzerosystems.com) for more information about InZero Corporation's technology. More information about the FIPS 140-2 standard and validation program is available at http://csrc.nist.gov/cryptval.

1.2 Supporting Documentation

This non proprietary *Security Policy* document addresses certain specific FIPS 140-2 requirements for security policy documentation. In addition to this document, the FIPS 140-2 Submission Package includes the following proprietary vendor evidence documents:

- Vendor Evidence Document, which contains the module's Finite State Model and addresses the vendor evidence requirements for FIPS 140-2 multi-chip standalone cryptographic modules.
- Hardware Design
- Other supporting documentation, as required.

Operators of the validated module may find more detailed operational information in the following supporting product documentation, included with each module shipment:

- *InZero Gateway Installation Guide*
- *InZero Gateway User Guide*
- *InZero Gateway Administration Guide*
- *InZero Security Platform Administration Guide*

2 Module Specification

The InZero Gateway XB2CUSB3.1 Series cryptographic module operates within a distributed architecture called the InZero Security Platform. The architecture consists of a Management Console, Management Server, and arbitrary numbers of FIPS and non-FIPS Gateways.

2.1 InZero Security Platform Architecture

The InZero Security Platform provides centralized management for multiple Gateways. The following figure shows the components of the InZero Security Platform for a small security domain.

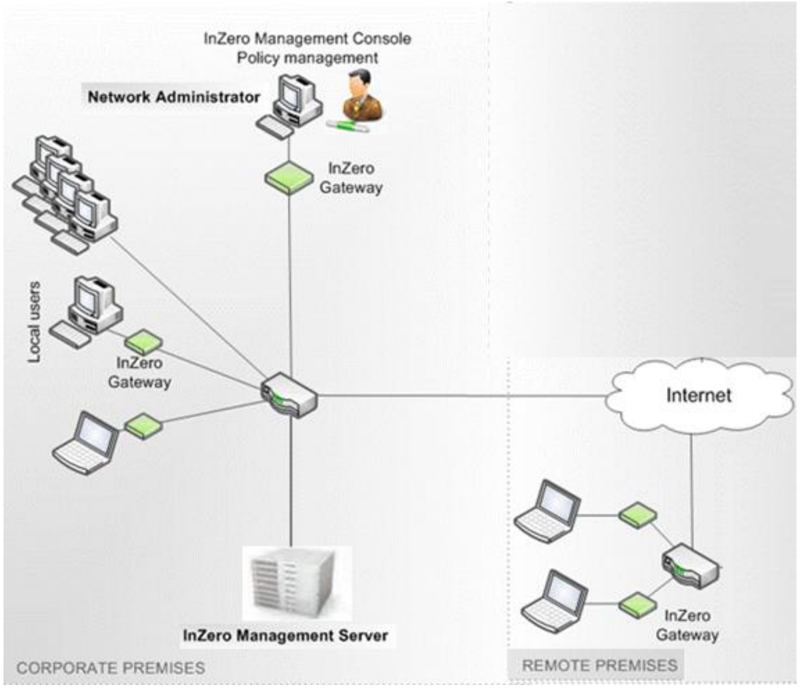


Figure 1 - InZero Security Platform

Network administrators install the InZero Management Console software on their PCs and use the Management Console software to configure Gateways, Policies, and Virtual Private Networks (VPNs). These administrative settings are stored on an InZero Management Server, which makes the settings available for Gateways to download.

2.2 Module Overview

The Gateway module protects against classes of malware attacks (known and unknown) and controls User and application network activity. It provides the following services:

- Hardware-enforced Application Sandbox provides a safe environment for opening dangerous content
- Firewall provides Network Access Control and limits propagation of malware
- Mail and web proxy services filter network data according to policy
- File conversion mechanism creates a sanitized copy of a malicious file
- Flexible management solutions (standalone, member of domain).

The module provides FIPS cryptography for operator authentication, policy management, VPNs, and InZero's XB2Pack file security container. The following module diagram illustrates the module's hardware, firmware, and connection to an Operator PC. It also illustrates the hardware ports and interfaces, described further in Section 2.7.

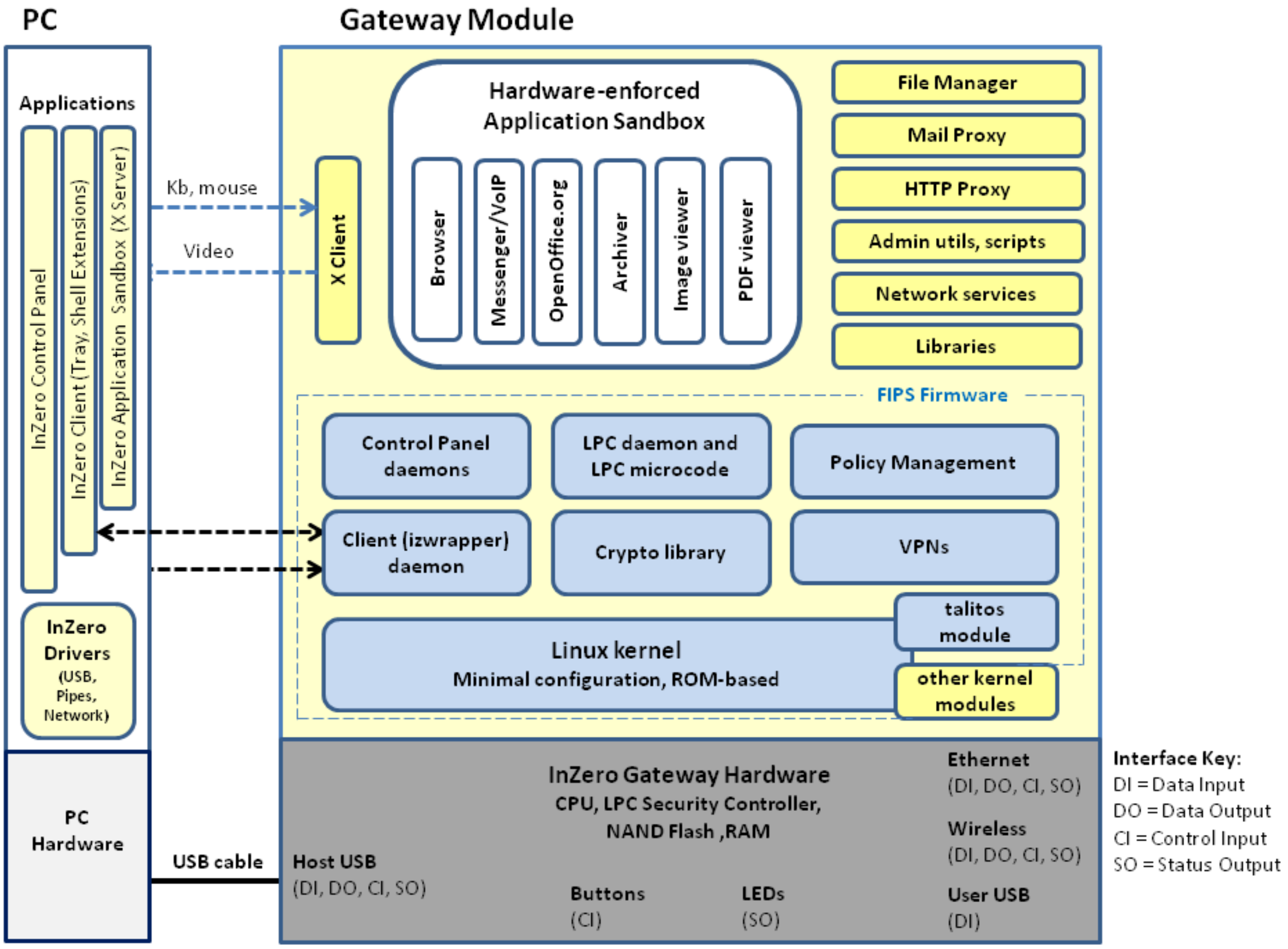


Figure 2 – Module Diagram

The Policy Management data flow (via Ethernet and Wireless DO/DI) is always encrypted. All other data flows are encrypted if they are routed to a VPN; otherwise, the data flows are plaintext or considered plaintext.

The module has three hardware boot modes that may be invoked with buttons on the top panel or by client software available on the tray icon menu. The current mode is indicated by a mode LED.

- When the module is booted in Ready mode (READY LED on), Users (but not the CO) may authenticate and access the module according to policy. Users may view (but not modify) configuration settings via the Gateway Control Panel.
- When the module is booted in Config mode (CONFIG LED on), Operators can perform certain changes to configuration data.
- Setup mode presents a USB drive with software to install the PC client and driver software.

2.3 Security Requirements

The InZero Gateway XB2CUSB3.1 Series is validated as a Level 2 multi-chip cryptographic hardware module. Table 1 lists the security level for each section of the FIPS 140-2 security requirements:

Table 1 - Validation Level by Section

Section	Level
Cryptographic Module Specification	2
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
Overall Level	**2**

2.4 Roles

The module supports the following required Operator roles.

- **Crypto Officer (CO) role**. The CO is responsible for overall management of the cryptographic module. The product documentation refers to this role as the Gateway's local administrator (**`admin`** account). The CO can login to **`admin`** account in Config mode only and cannot send or receive any data via the module or access any files on the module. The CO is limited to using the module's Control Panel in Config mode to change the module's configuration, manage the module's keys, review audit logs, and manage User accounts. The CO is also responsible for physical security of the module.
- **User role**. Users can perform communications functions and data storage operations when the module is in Ready mode. The module supports as many as five User accounts, with only one User logged in at a time. Users can perform network operations, store data in a dedicated personal folder (InZero Disk) on the module, and use the Control Panel to view the configuration.

The module does not support concurrent Operators or a Maintenance role. Unauthenticated persons may view the module's status LEDs and operate the module's buttons (e.g., turn power on or off). Except for these unauthenticated services, no Operator may access the module's services without authenticating to the module. An operator cannot change identity or role without exiting the current session (logging out or shutting down the module) and authenticating.

The InZero Security Platform provides an additional **Network Administrator role** that does not interact directly with the module but does configure the policy, VPN, and other settings the module downloads from the

Management Server. The network administrator's functions are described in the *InZero Security Platform Administration Guide*.

2.4.1 Authentication

The Gateway module performs authentication for the following operator roles. Passwords may be up to 31 characters long and use mixed-case alphabetic, numeric, and non-alphanumeric ASCII characters.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
CO	Role-based	Password (8 or more characters, minimum strength **Good**)
User	Identity-based	Password settings configured by Network Administrator: • Minimum password length. Section 4.1 (Secure Operation) explains that the module must be configured for a minimum User password length of 6 characters. • Minimum password strength **Good** (Recommended) • Password lifetime restrictions (optional) • Lockout mechanism to deter password guessing (optional)

The PC's client software displays a graphical login prompt, reads the password (displaying a round dot for each character typed), and transfers the credentials to the module's USB interface for authentication. When the module is powered off and subsequently powered on, the results of previous authentications are not retained and the module requires the operator to be re-authenticated.

Table 3 presents the minimum strength results for password and certificate-based authentication mechanisms using random authentication credentials:

Table 3 - Strength of Authentication Mechanisms

Authentication Mechanism	Assumptions	Strength of Mechanism	To Increase Strength
Password-based (Operator)	• Six random lowercase characters (User)	1 in 26^6 (one in 308 million is stronger than one per million)	• Use longer password • Use mixed case, numeric and punctuation
Certificate-based	• Minimum RSA key size of 1024 bits provides 80 bits strength	1 in 2^{80} (one in a 2^{80} is stronger than one per million)	• Use 2048-bit keys (112 bits strength)

2.5 Services

Table 4 lists the cryptographic services provided by the module and maps access to these services to roles and to the module's modes of operation. The numbers in the Keys & CSPs column refer to Table 10. Write (W) access implies Sanitize. There is no Execute access.

Table 4 - Services Mapped to Roles

#	Service	Role(s)	Keys & CSPs	RW	Boot Mode	Description
1	Initialization	Unauthenticated	n/a	n/a	Ready, Config	Power-on self test occurs when the Gateway module finishes booting.
2	Self test	CO, User, Unauthenticated	n/a	n/a	Ready, Config	An Operator can run self tests by pressing and holding the Function (**Fn**) button on the Gateway's top surface for 5 seconds.
3	Show Status	User, CO, Unauthenticated	n/a	n/a	Ready, Config	The LEDs provide the Show Status command (see Section 2.7). A User or CO may also open the Gateway Control Panel Summary tab in Ready or Config modes to display the module's cryptography mode, VPN status, and the FIPS firmware fingerprint.
4	Module Configuration	CO	n/a	n/a	Config	A CO can use the Gateway Control program to configure the module.
5	Manage Module Passwords	CO, User	CO: 1,2 User: 2	W	Config	The CO can set CO and User passwords and authentication settings. If permitted, Users can change own passwords.
6	Open VPN Session	User	3, 5	n/z	Ready	Users can open any previously configured VPN interface by accessing a network resource that uses the interface.
7	Read/write *InZero Disk* on module	User	n/a	n/a	Ready	User can store files on module (download via browser, upload from PC), open files, and transfer files to PC. Open Windows Explorer.
8	Key Management	CO	3, 4	RW	Config	The CO can use the Gateway's Control Panel Domain/PKI tab to generate or import the module's Network and Configuration key pairs.
9	Open management connection	CO	3	R	Ready	The Gateway Policy Management Agent opens the HTTPS management connection to the Management Server, checks for policy updates, and downloads and installs the update if required.

#	Service	Role(s)	Keys & CSPs	RW	Boot Mode	Description
10	Define Network interface settings	CO, User	n/a		Config	The Network Administrator (Management Console) can define physical network configurations for the module's Ethernet, Wireless, and USB interfaces. The CO or User can view or modify these settings on the Gateway's Control Panel. (These changes are uploaded to the Management Server.) VPN settings cannot be modified by the User.
11	Define Domain settings	CO	n/a	n/a	Config	The CO must log in to the module, open the Control Panel "Domain/PKI" tab, select **Member of domain** and define the Management server address.
12	Define Management settings	CO	n/a	n/a	Config	CO can reset partitions, create User accounts, manage User rights, set system date/time, review and delete audit logs, and import/export settings.
13	Install client software on PC	CO, User, Unauthenticated	n/a	n/a	Setup	This is the software that virtualizes the User's interactions with the module and manages the USB interface to the module. This software does not enforce security.
14	Change mode	CO, User	n/a	n/a	Any	Mode can be changed with **MODE** button on top of module.
15	Confirm data transfer or configuration changes	CO, User	n/a	n/a	Config or Ready	Confirm an action by pressing the **OK** button when prompted.
16	Zeroize module	CO, unauthenticated	1, 2, 3, 4	W	Config	Overwrite keys, CSPs, and other module settings with the factory default settings.
17	Provide entropy for RNG	CO, User	n/a	n/a	Config, Ready	The ANSI X9.31 RNG reads entropy from /dev/random.
18	Update firmware	CO, User	n/a	W	Config	The module reboots in Config mode with firmware update permission, verifies the update's digital signature, and installs the new firmware.

In a domain configuration, a Network Administrator can define the following module settings at the Management Console (Figure 1). The module downloads these settings (Service 9, Open Management Connection) from the Management Server.

- **VPN Interfaces.** The Network Administrator can only select FIPS-approved cipher and integrity algorithms for FIPS modules, but the choice of algorithms is enforced by the Gateway module. For external VPNs, the Network Administrator may specify the password and pathname for an external key.
- **Policy settings**. Policy settings include Network/Firewall, Application Sandbox, Data Transfer, Services/Proxies, and user authentication. Users and COs can use the Gateway Control Panel to view, but not modify, these settings.
- **Network interface settings**. The Network Administrator can define physical network configurations for the module's Ethernet, Wireless, and USB interfaces. The CO or User can view or modify these settings on the Gateway's Control Panel. Users cannot modify VPN settings.

2.6 Cryptographic Boundaries

The InZero Gateway is a network security device that connects the Operator's PC to the internet. The physical cryptographic boundary is defined as encompassing the external surfaces of the case, shown below. The physical boundary does not encompass the module's power supply or external cables.

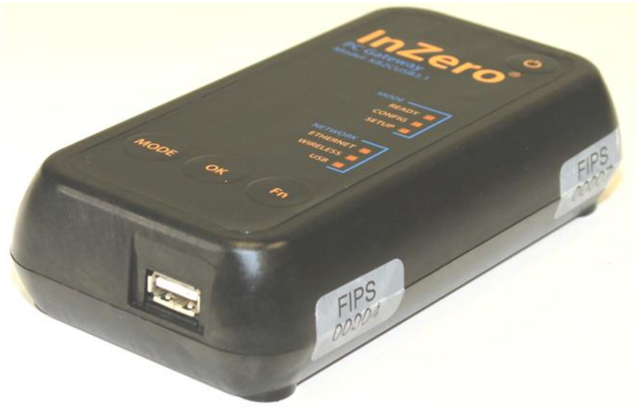


Figure 3 - Cryptographic Boundary

The FIPS firmware residing inside the physical boundary includes the SSL library, authentication, VPN, and management functionality. The module maintains and checks a cryptographic fingerprint of this firmware as part of the module's self tests. The module's sandbox applications (e.g., browsers, office applications, and file viewers) are excluded from the module and do not have unprotected access to keys or CSPs in the module.

2.7 Ports and Interfaces

The Mode and Network LEDs indicate the Gateway's status. LEDs blink sequentially during self-tests.

The **MODE** LEDs indicate the Gateway's current operating mode. Only one LED will be on solid at any time, but the Gateway may blink all three LEDs during mode changes. If a mode LED is flashing by itself, it indicates that the Gateway is preparing to boot into that mode or is shutting down after being in that mode.

Network LEDs indicate the use of a specific network interface. Multiple network LEDs may be activated at once, depending on which interfaces are configured.
A self-test failure is indicated by blinking all three LEDs in unison.

These LEDs provide the module's Show Status service:

Booting: selected MODE LED blinking
Operating in FIPS Ready mode: READY LED on, one or more NETWORK LEDs blinking
Operating in FIPS Config mode: CONFIG LED on
Running self-test: all LEDs blinking sequentially, one at a time
FIPS self-test error indication: all NETWORK LEDs blinking in unison.

The Gateway module has four control buttons on the top surface. The Power button is located at the upper right of the Gateway faceplate, and the remaining three buttons are on the bottom edge of the faceplate:

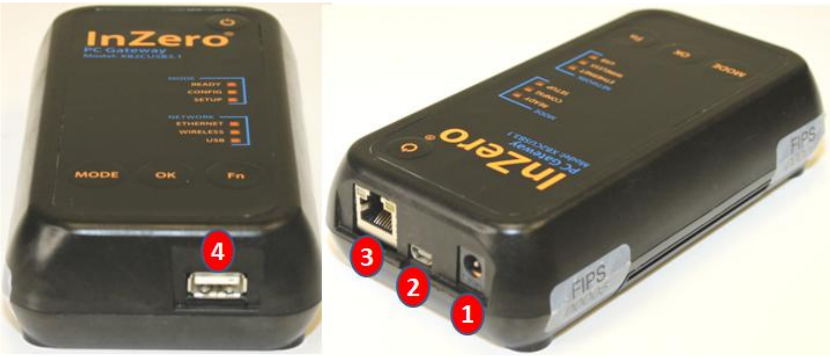
Press the Power button is used to turn the Gateway off (e.g., before unplugging power) or to awaken the Gateway from sleep. The Gateway blinks all six LEDs after you press and hold the Power button, and then turns off all LEDs when the shutdown is complete.

MODE Press the **MODE** button to select a new boot mode. The MODE LEDs will cycle from READY to CONFIG to SETUP. The selected LED will flash while module is booting and then go on solid.

OK Press the **OK** button to confirm configuration changes and data transfers.

Fn Use the Function button (**Fn**) for certain administrative and User functions, including performing a FIPS self-test and requesting an update from the Management Server.

The Gateway module has the following physical interfaces:



Port ❶ provides 5 volt DC power from external supply (3 ampere capacity).

Port ❷ (USB 2.0 mini) is the Gateway's interface to the PC.

Port ❸ is the gigabit Ethernet interface (RJ-45).

Port ❹ (USB type A) is the User USB interface. It may be used to import external RSA keys.

Figure 4 - Physical ports

Two wireless antennas (not shown) are located underneath the top surface. This interface is considered plaintext.

The physical interfaces provided by the Gateway module are mapped to four defined logical interfaces: data input, data output, control input, and status output. The network interfaces (Ethernet, Wireless, and PC USB) all provide data input and control input and generate data output and status output. All buttons generate control input and all LEDs generate status output.

Table 5 - Ports and Interfaces

Physical Port and Interface	**Data Input**	**Data Output**	**Control Input**	**Status Output**	**Power**
Port ❶ (power jack)					X
Port ❷ (PC USB, USB mini)	X	X	X	X	
Port ❸ (Ethernet)	X	X	X	X	
Port ❹ (User USB, Type A)	X				
Wireless interface	X	X	X	X	
Buttons (Power, MODE, OK, Fn)			X		
Mode LEDs (Ready, Config, Setup)				X	
Network LEDs (Ethernet, Wireless, USB)				X	

2.8 Self-Tests

The module self-tests that are run automatically during the Gateway boot sequence (Power-up tests, Table 7) and manually (on demand) while the module is running to ensure the module is functioning correctly. The module must pass all self-tests before an Operator can perform any subsequent cryptographic services.

An Operator can initiate self-tests on-demand by pressing and holding the Function (**Fn**) button on the top surface of the module (see Section 2.4) for 5 seconds. Regardless of how the self-test is initiated, it indicates its status with the following LED patterns:

- The module stops all running network interfaces and displays a cyclic LED pattern (one LED at a time) while it is running the test.
- When the module passes the self-test, it restarts any stopped network interfaces and displays the normal LED pattern. In Ready mode it displays the READY LED (on continuously) and one or more Network LEDS. In Config mode it displays the CONFIG LED on continuously with no Network LEDs.
- Otherwise, if the module does not pass the self-test, the module audits the failure, indicates an error by blinking all network LEDs (Ethernet, Wireless, and USB) in unison and removing the tray icon. It is not possible to restart any network interfaces without rebooting the Gateway module.

Some error conditions may be cleared by pressing the Power button to shut down the module and pressing the Power button again to reboot the module.

The module performs the power-up self-tests listed in Table 6. The algorithm tests are also run each time a process loads the cryptographic library. As described in Section 2.7, the module blinks all three network LEDs in unison (module self-test error indicator) if one of these tests fails.

Table 6 - Power-up Self-tests

Test	Method	Failure Indication
AES	KAT	Module self-test error indicator
Triple-DES	KAT	Module self-test error indicator
DSA	Pairwise consistency test, sign/verify	Module self-test error indicator
RSA	KAT	Module self-test error indicator
PRNG	KAT	Module self-test error indicator
HMAC-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	KAT	Module self-test error indicator
SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	KAT	Module self-test error indicator
Module integrity	HMAC-SHA-1	Module self-test error indicator

The module performs the following conditional self-tests (Table 7).

Table 7 - Conditional Self-tests

Test	Method	Failure Indication
DSA	Pairwise consistency	Module self-test error indicator
RSA	Pairwise consistency	Module self-test error indicator
PRNG	Continuous test	Module self-test error indicator
Firmware update (Config mode only)	The firmware update wizard calculates a digital signature using its CA certificate and compares the result with the required signature in the update.	Error screen indicating that digital signature is incorrect. Cryptographic processing is not possible until the Operator exits the wizard.

Operators may also run self tests from the Control Panel **System management > Diagnostics > FIPS** menu as described in Section 4.6.

2.9 Physical Security

InZero installs four numbered tamper-evident seals and an opacity shield before shipping the module. Any attempt to open the module will damage the seals, the opacity shield, or the material of the module's case. Upon receiving the module, the CO should record the numbers printed on the four seals. The CO should periodically inspect the seals and opacity shield to verify they are intact.

Table 8 - Inspection of Physical Security Mechanisms

Physical Security Mechanism	Recommended Frequency of Inspection	Inspection Guidance
Four tamper-evident seals (1 ¼" x 5/8")	Weekly	Signs of tampering include curling, crinkling, rips, slices, scraping, blistering, a crisscross pattern, or different number(s).
Opacity shield installed over air vents (left side)	Weekly	Signs of tampering include cracks, missing portions of the shield, or absence of the shield.

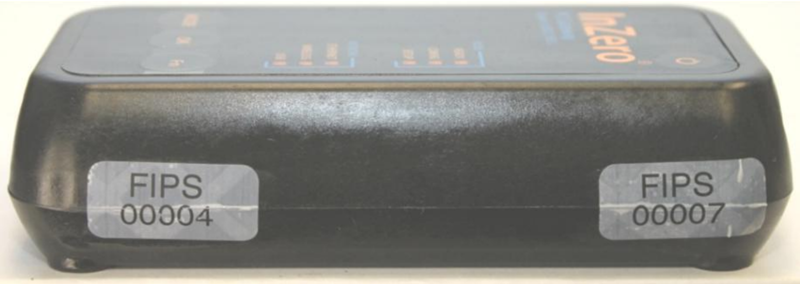
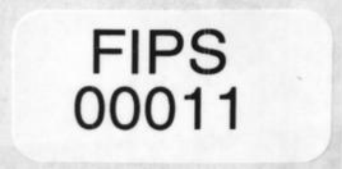


Figure 5 - Placement of Right-side Seals

InZero applies two numbered tamper-evident seals on each side of the module near the corners.



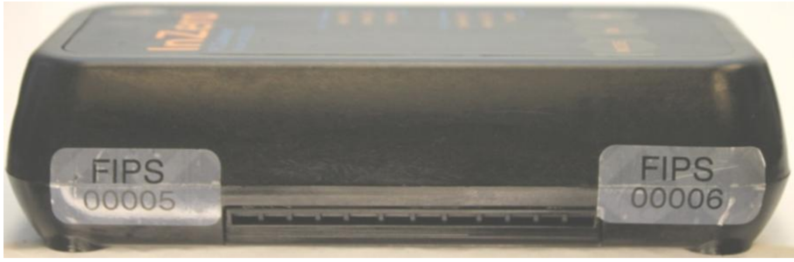


Figure 6 - Placement of Left-side Seals and Shield

The left side of the module has two more tamper-evident seals and an opacity shield covering the air vents.

The shield is a custom part of the FIPS Gateway that cannot be removed without obvious damage to the shield itself.

2.10 Mitigation of Other Attacks

The Gateway modules do not claim to mitigate any attacks in a FIPS-approved mode of operation.

3 Cryptographic Key Management

3.1 Algorithms

The Gateway module supports the following FIPS approved algorithms.

Table 9 - Approved Algorithms

Algorithm	Usage	Keys/CSPs	Notes	Certificate
AES	Encrypt/decrypt	AES keys 128, 192, 256 bits		1841
TDES	Encrypt/decrypt	3-key Triple-DES only (168 bits)	2-key 3DES excluded by policy	1194
PRNG (ANSI X9.31 Appendix A.2.4 using AES)	Random number generation	PRNG seed value is 128 bits; seed key value is 256 bits	Deprecated, see note.	967
RSA (X9.31, PKCS #1.5, PSS)	Sign and verify	RSA keys 1024, 1536, 2048, 3072, 4096 bits	1024 bits deprecated for signature generation, legacy use for signature verification (2011-2013).	929
DSA	Sign and verify	DSA keys 1024 bits	1024 bits deprecated	576
SHA-1 SHA-224 SHA-256 SHA-384 SHA-512	Hashing	n/a	SHA-1 is deprecated for digital signature generation, legacy use for digital signature verification.	1622
HMAC-SHA-1 HMAC-SHA224 HMAC-SHA256 HMAC-SHA384 HMAC-SHA512	Message integrity	HMAC key		1095

The Gateway module supports the following algorithms that are allowed in FIPS mode for key agreement and key establishment, even though they are Non-Approved for that purpose:

- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength).

3.2 Key Generation

The Gateway module supports generation of RSA, DSA, and Diffie-Hellman public/private key pairs.

- The module generates RSA keys for authentication of the module (Network key) and for signing and verifying the module's configuration (Config key). The Network key pair can also be imported from a USB drive connected to the module. The module also supports import of externally-generated VPN client keys from USB drives. The module does not generate DSA keys except for test vector processing.
- Diffie-Hellman is used to generate session keys for VPN traffic when a VPN starts and as specified by VPN key change parameters.

The module provides an ANSI X9.31 compliant pseudo-random number generator to perform key generation and uses those keys directly without further modification. The PRNG is seeded from /dev/random, which gathers entropy from Linux events and from the CPU via Talitos driver.   This provides the PRNG with 256 bits of entropy for the seed key (estimated strength 256 bits) and 128 bits for the seed value (estimated strength 128 bits).

> **Note:** The ANSI X9.31 PRNG is listed by NIST SP 800-131A as deprecated from 2011 through 2015. This deprecated status requires the User to assume some risk regarding its usage. As described in the following section, random numbers are used to generate keys (primarily VPN traffic keys) so the issue is whether a weak random number makes it easier to attack key generation than the algorithm itself.
>
> As the designated end date (December 31, 2015) approaches, the level of risk becomes higher. This risk is reduced somewhat because the Gateway module does not permit an attacker to directly request random numbers or observe the processes running on the Gateway module that are generating the input entropy for the PRNG.

3.3 Key Storage

The Gateway module supports the following types of key storage.

1. The module's RSA Network and Config keys are stored inside a hardware device that can be accessed only by the operating system. These keys are not exposed to any external interface and cannot be viewed by the CO or User. These keys can be zeroized by generating a new key.
2. VPNs can be configured to use externally generated RSA keys loaded from a USB drive plugged in to the module. The USB drive must be mounted for the VPN to restart. The CO must manually sanitize the key pair.
3. The module automatically generates session keys when they are required, for example, during VPN connection and key change processing. These keys are maintained in RAM within the network process and are zeroized when the keys are released by the appropriate API function calls. The process does not perform persistent storage of session keys.

3.4 Key/CSP Access, Protection and Zeroization

Gateway modules use the following keys and Critical Security Parameters (CSPs) during operation. Table 10 lists the cryptographic keys and CSPs.

Table 10 - Keys and CSPs

#	Key/CSP Name	Algorithm	Description	Source, Storage, Export	Zeroization
1	CO Password	Shared secret (8-31 characters, minimum strength **Good**)	Used to authenticate CO. Password is encrypted with Network public key for transfer from PC to Gateway.	Read from PC USB channel (encrypted by PC). Stored in RAM as plaintext and hash. Long term storage in auxiliary CPU as SHA-256 hash. Cannot be exported.	Memory: Plaintext zeroized after it is hashed. Long term-hash is overwritten by new password or resetting to factory defaults.
2	User Passwords	Shared secret (6-31 characters, minimum strength **Good**)	Authenticate a User. Password is encrypted with Network public key for transfer from PC to Gateway.	Read from PC USB channel (encrypted by PC). Stored in RAM as plaintext and hash. Long term storage in system file as SHA-256 hash. Cannot be exported.	Memory: Plaintext zeroized after it is hashed. Long term-hash overwritten by new password or resetting to factory defaults.
3	RSA Network private key	ANSI X9.31/RSA	Key used for networking. Protects CO and User passwords, VPN keys, and WiFi passwords. Module generates 2048 bit keys, can import 1024, 1536, and 2048 bit keys.	Key pair is generated by module or imported. Stored in auxiliary processor. Cannot be exported.	See Section 3.3: Key can be zeroized by overwriting when CO generates new key, resetting to factory defaults, or changing to Standalone mode.

#	Key/CSP Name	Algorithm	Description	Source, Storage, Export	Zeroization
4	RSA Config private key	ANSI X9.31/RSA	Key used to sign and verify configuration files. The module generates 2048 bit keys.	Key pair is generated by module. Stored in auxiliary processor. Cannot be exported.	Key can be zeroized by CO generating new key or resetting configuration.
5	RSA External private keys	ANSI X9.31/RSA	Network key used for external VPN. Module accepts 1024 (deprecated), 1536, 2048, 3072, and 4096 bit keys.	Key pair is generated by external CA and imported on USB drive (PEM, PKCS#8, or PKCS#12 format). Key cannot be exported by module.	External keys must be manually zeroized by CO.
6	SSL, TLS session keys	ANSI X9.31 3DES, AES DH	Exchanged using public/private key pairs.	RAM (plain text). Cannot be exported.	Session keys are changed according to VPN Change Key parameters. Zeroized by VPN or module shutdown.
7	PRNG Seed Data	Entropy	Seed data for X9.31 PRNG is read from /dev/random.	Plain text read from kernel memory into process space. Cannot be exported.	Each value is overwritten by next read. Turn off or reboot Gateway.

4 Secure Operation

This section describes how to operate the module in a FIPS-approved mode throughout its life cycle.

The module is in a FIPS-approved mode when it is booted in Ready mode or Config mode and the boot self-test is successful. This is indicated by the corresponding mode LED (READY or CONFIG) on solid. The module remains in FIPS mode until a subsequent self test fails or the module is shut down.

4.1 Module Initialization (CO)

The CO is responsible for receiving, installing, and initializing the Gateway module as well as for the continued operation of the module. InZero delivers modules via conventional delivery services (such as FedEx, DHL, or USPS), via a bonded courier of the customer's choice, or by direct pickup at InZero's facilities. See Section 3 of the InZero Gateway Installation Guide for more information on site preparation, checking the shipment for damage, and hardware installation.

Before proceeding, the CO should check the four factory-installed tamper-evident seals and record their numbers as described in Section 2.9. The CO must perform the following steps to prepare the Gateway module and configure it for a FIPS-approved mode of operation.

4.1.1 Installing the Module

All step number references in this section are with respect to the printed *InZero Gateway Quick Installation Guide* in the Gateway box.

1. Connect the Gateway module to PC as shown in Step 1 of the instructions.
2. Boot the Gateway module in Setup mode (Steps 2 and 3) and install the InZero Software Suite and product documentation PDFs on your PC (Step 4).
3. Reboot the Gateway module in Config mode (Step 6). Log in as **`admin`** with the factory default password and start the Control Panel as described in Step 7.

4.1.2 Reset Module to Factory Defaults

Follow the instructions in Section 8.1.2.2 of the *InZero Gateway Administration Guide* to reset the module's RSA keys, passwords, and module configuration to factory default. This is the only FIPS approved method for zeroizing the module.

4.1.3 Generate Configuration Key

Log in as **`admin`** and start the Control Panel. Open **Domain/PKI > PKI settings > Gateway configuration key** menu to generate a new configuration key pair, as described in Section 7.2.4 of the *InZero Gateway Administration Guide*.

4.1.4 Configure Module for Domain Management

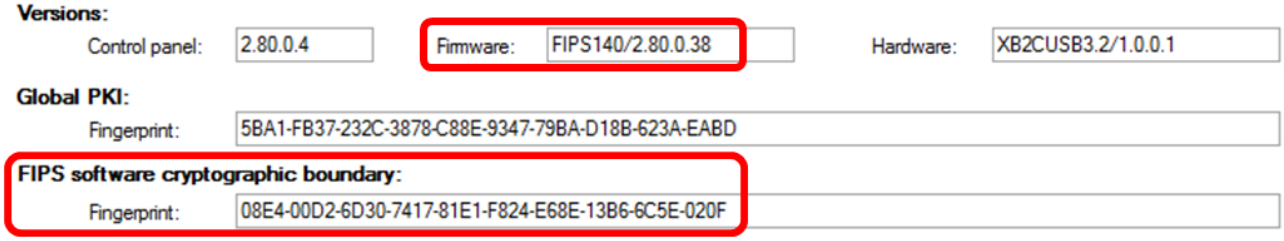
Open **Domain/PKI->Domain Settings->Domain Membership** tab to configure the Gateway module as **Member of Domain**. Open the **Management servers** menu and define the Management Server address and port. See Section 7.1 of the *InZero Gateway Administration Guide* for more information.

4.1.5 Generate Network Key (Optional)

Configuring the module for domain management automatically generates a new RSA Network key pair. You may optionally use the **Domain/PKI > PKI settings > Gateway certificate** menu to generate a different key. See Section 7.2.3.1 of InZero Gateway Administration Guide. A new certificate can be downloaded later, during registration with your Management Server.

4.1.6 Verify Firmware Version and FIPS Fingerprint

Open the Gateway's Control Panel **Summary** tab and scroll down to the bottom to verify that your module is running the approved **FIPS140/2.80.0.38** firmware and has the same **FIPS Fingerprint** (integrity value) for the FIPS firmware running on the module. If your module's **Firmware** or **FIPS Fingerprint** is different, then the module is not running the FIPS-approved firmware.



Versions:

Control panel: 2.80.0.4
Firmware: FIPS140/2.80.0.38
Hardware: XB2CUSB3.2/1.0.0.1

Global PKI:

Fingerprint: 5BA1-FB37-232C-3878-C88E-9347-79BA-D18B-623A-EABD

FIPS software cryptographic boundary:

Fingerprint: 08E4-00D2-6D30-7417-81E1-F824-E68E-13B6-6C5E-020F

As described in Section 4.6, you may also check the FIPS fingerprint from the Control Panel's **System Management > Diagnostics > FIPS** menu.

4.1.7 Configuration Changes

The following administrative settings are required for the module to comply with FIPS requirements:

- Network Administrator must configure **Policy > Data exchange > File exchange > General > USB storage mode** to **Key Storage Only** to prevent external keys used for FIPS VPNs from being imported by protected browser. (See Section 11.3.3.1.1 of *InZero Security Platform Administration Guide*.)
- Network Administrator must select **Require user login to activate network** on Network/VPN tab. (See Section 11.4 of *InZero Security Platform Administration Guide*.)
- CO must open Control Panel **System management > User management > User accounts** tab and change the password for `user` account. (See Section 8.3.2 of *InZero Gateway Administration Guide*.)

4.1.8 Change CO Password

Right click the Gateway module's tray icon and select **Log out (Config mode)**.

Right click the Gateway's tray icon and select **Log in (Config mode)**. Enter the **Username `admin`**, the current (default) password, and click **Change Password**. Change the factory default **`admin`** password as described in Section 2.2 of the *InZero Gateway Administration Guide*. The module requires at least an eight character password with strength **Good** for the **`admin`** account.

These will be the only changes required with the Gateway Control Panel to initialize the Gateway for FIPS mode operation. After placing the Gateway in domain mode, the Gateway will register with the Management Server (see Chapter 6 of the *InZero Security Platform Administration Guide*).

4.2 Managing External Keys (CO)

In addition to the internal Network key, the Gateway module also allows use of externally-generated RSA keys for VPNs. Available key sizes are 1024 bits (deprecated), 1536, 2048, 3072, and 4096 bits. FIPS VPNs cannot be started with key sizes smaller than 1024 bits. External keys are read from a USB drive plugged in to the module. The assigned User is responsible for securing the key. The USB drive can be removed after the VPN starts, but the VPN will not restart (e.g., after a self-test) unless the USB drive is plugged in. USB key storage has certain obvious physical security disadvantages. If the USB drive is not plugged in or the key is inaccessible, the module will generate an audit event once each minute while it is waiting.

Gateways may have up to five Users total. VPNs are per-Gateway, not per-User, so if there are multiple Users on the Gateway, they will all have access to the VPN while the key is installed. The best way to provide individual accountability is to assign only one User to each Gateway.

4.3 Module Configuration (CO)

Subsequent definition of VPNs, Gateway security policy, and other settings (defined in the *InZero Security Platform Administration Guide)* will be defined by a Network Administrator at an InZero Management Console. The Management Console saves the configuration to an InZero Management Server. Gateway modules then poll the Management Server download the configuration data whenever there are changes. The CO's responsibilities in this process are as follows:

1. Communicate FIPS security requirements to the Network Administrator. These include VPN configurations (e.g., FIPS, PKI, cipher, integrity, and key change) and User password requirements.
2. Run the module's Control Panel (*InZero Gateway Administration Guide*) to verify that the module is properly configured. VPN settings can be viewed but not changed on the **Network/VPN** tab (Chapter 6). User and password settings are displayed on the **System management > User management > User accounts** tab (Section 8.3). Policy settings are displayed on the **Policy** tab (Chapter 5).

4.4 Configuring FIPS Mode VPNs (Network Administrator)

InZero's FIPS Gateways provide a protected hardware environment for implementation of Secure Socket Layer (SSL) VPNs. As described in Chapter 10 of the *InZero Security Platform Administration Guide*, a Network Administrator can use the Management Console to create internal (Gateway to Gateway) or external (Gateway to server) VPNs. A Network Administrator adds Gateway VPN servers in the **VPN** tab with a few menu selections and then drags Gateway clients into the VPN.

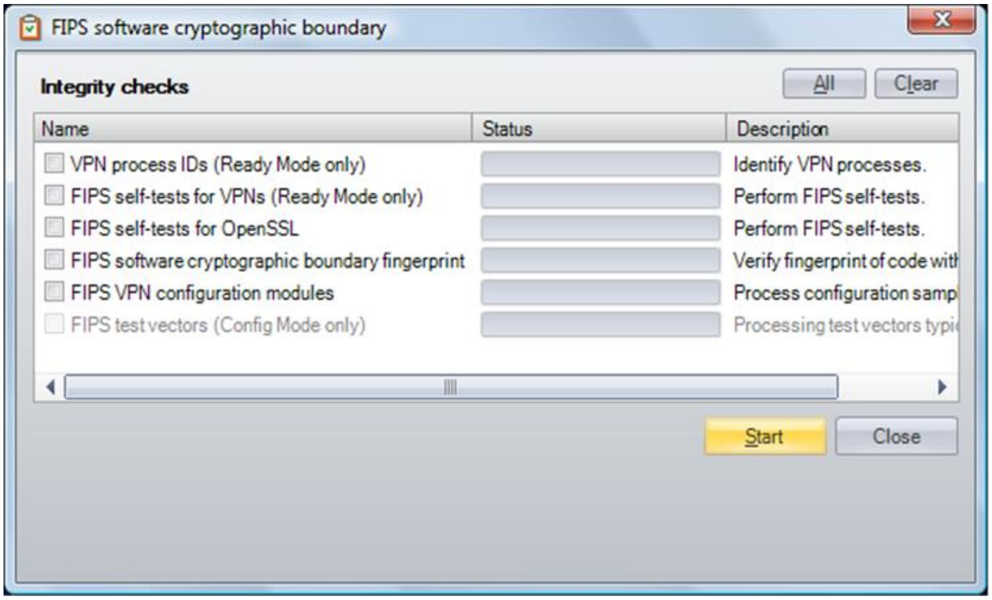
Section 6.2.4 of the *InZero Gateway Administration Guide* describes how the CO can create VPN client connections for standalone Gateway modules to external VPN servers.

4.5 Zeroizing the Module (CO)

The CO can zeroize the module as described in Section 8.1.2.2 of the *InZero Gateway Administration Guide*). This is the only FIPS approved method for zeroizing the module.

4.6 Diagnostics (All Operators)

The CO or User may run diagnostic tests as required by opening the module's Control Panel **System management > Diagnostics > FIPS** menu.



Name	Status	Description
□ VPN process IDs (Ready Mode only)		Identify VPN processes.
□ FIPS self-tests for VPNs (Ready Mode only)		Perform FIPS self-tests.
□ FIPS self-tests for OpenSSL		Perform FIPS self-tests.
□ FIPS software cryptographic boundary fingerprint		Verify fingerprint of code witl
□ FIPS VPN configuration modules		Process configuration samp
□ FIPS test vectors (Config Mode only)		Processing test vectors typi

Select one or more tests and click **Start**. Tests (e.g., **FIPS test vectors**) may be disabled and cannot be selected if the module is in an inconsistent mode, e.g. Ready versus Config mode.

For each test, the Control Panel displays Done in the **Status** column if the module passes the test and displays an error indicator on a red background if the module fails that test.

The **FIPS** menu provides the following diagnostic tests. Selecting items 3, 4, and 5 is equivalent to pressing the **Fn** button for five seconds to run the power-up self-tests.

1. In Ready mode, the **VPN Process IDs** tests all running VPN processes and checks the software version, FIPS mode, and status. (The test is unavailable in Config mode.)
2. In Ready mode, the FIPS self-tests for VPNs runs the SSL algorithm tests within each running VPN process.
3. The **FIPS self-tests for OpenSSL** item runs the SSL algorithm tests listed in Table 6, excluding the module integrity self-test.
4. The **FIPS software cryptographic boundary fingerprint** performs the module integrity self-test as indicated in Table 6 and described in Section 4.1.6.
5. The **FIPS VPN configuration modules** test verifies that the module properly unpacks and converts an XML configuration file received from the Management Server to a VPN configuration file.
6. In Config mode, the **FIPS test vectors** test is provided primarily for the validation laboratory to validate the module's algorithm implementation. Customers who have test vectors should contact InZero for procedures on using this interface. (This test is unavailable in Ready mode).