Confidence in Wireless Networks™

ReefEdge, Inc.
Edge Controller 100x

(Hardware Version 3.0, Software Version 3.1.3)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation
Version 0.80

August 2003

Table of Contents

Introduction

Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Edge Controller 100x from ReefEdge, Incorporated (ReefEdge). This security policy describes how the Edge Controller 100x meets the security requirements of FIPS 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/cryptval/.

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 ReefEdge website http://www.reefedge.com/ contains information on the full line of products from ReefEdge.

- The NIST Validated Modules website (http://csrc.nist.gov/cryptval/) contains contact information for answers to technical or sales-related questions for the module.

Document Organization

The Security Policy document is one document in a complete FIPS 140-2 Submission Package. In addition to this document, the complete Submission Package contains:

  - Vendor Evidence document
  - Finite State Machine
  - Other supporting documentation as additional references

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

REEFEDGE EDGE CONTROLLER 100x

Overview

ReefEdge Connect integrates wireless access points, networking, and IT management infrastructure to build enterprise-grade wireless local area network (WLAN) systems. The Connect system delivers a WLAN with comprehensive security, cross-subnet mobility, and manageability—all with the quality, reliability, and scalability expected by mid- to large-sized organizations.

The Connect system acts as a distributed firewall and VPN, protecting the corporate network from hackers. All wireless users can be required to authenticate to the Connect system, either through a standard web browser or through the ReefEdge Mobile Domain Utility, and then transparently authenticate to the Edge Controller module to securely access the corporate network. The privileges of different classes of users can be limited through access control rules and quality of service (QoS) policies.

The ReefEdge Edge Controller 100x, a member of the ReefEdge family of Edge Controllers, provides perimeter security and high-speed subnet roaming to the ReefEdge Connect System, connecting an enterprise's access points to its wired LAN. The Edge Controller 100x enforces access control rules, implements bandwidth management, and performs encryption, enabling users to roam freely- among offices, between floors, across campuses-without losing their secure connection.

The Edge Controller 100x meets all level 2 FIPS 140-2 requirements.

Area	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
Electromagnetic Interference/Electromagnetic Compatibility	2
Self-tests	4
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 1 – Validation Level

Module Interfaces

The cryptographic boundary of the EC100x is defined as the metal case enclosing all of the system components. The module is accessible only through well-defined physical ports, including an internal Ethernet port (connected to the LAN), an external Ethernet port (connected to the WLAN), LEDs, a serial port, a power switch, and a power connector. (The module has two additional Ethernet ports and one additional serial port. These ports are not initialized or used in the FIPS-compliant version of the EC100x.)

Figure 1 – Physical Ports of the Module

All of these physical ports are separated into the logical interfaces defined by FIPS 140-2, as described in the following table:

Module Physical Ports	FIPS 140-2 Logical Interface
Ethernet ports, Serial port	Data Input Interface
Ethernet ports, Serial port	Data Output Interface
Ethernet ports, Serial port, Power switch	Control Input Interface
Ethernet ports, Serial port, Indicators	Status Output Interface
Power connector	Power Interface

Table 2 – FIPS 140-2 Logical Interfaces

Roles and Services

The module supports role-based authentication. There are three roles in the module that operators may assume: a Local Crypto-Officer role, a Crypto-Officer role, and a User role.

The Local Crypto-Officer accesses the module using a command line interface (CLI) over the serial port. The operator authenticates with a password and is able to perform minimal configuration of the module.

The Crypto-Officer accesses the module through the internal Ethernet port over a session secured with IPSec. The operator authenticates during a TLS handshake using RSA and per packet using a shared secret SHA-1

HMAC key. The Crypto-Officer has the ability to fully configure and manage the module.

The User role accesses the module using IPSec-secured communications through the external Ethernet port. The User authenticates per packet using a shared secret SHA-1 HMAC key. Additionally, the User role can also transfer specific packets through the module in plaintext (bypass), without IPSec processing.

Local Crypto-Officer Role

The Local Crypto-Officer is responsible for the initial, minimal configuration of the module. This configuration involves setting the Local Crypto-Officer password, configuring the management server information, and establishing network settings for the module.

The Local Crypto-Officer is able to access minimal configuration settings and has the ability to view a variety of status information.

The following table details the Local Crypto-Officer's set of services in FIPS mode.

Service	Description	Input	Output
Config	Configuration of network settings, management server information, password, and enable/disable FIPS mode of operation	Command, password, and necessary configuration information	Status of command and configuration information
Default	Return module to default settings	Command and password	Status of command
Halt	Stop operation of the module	Command and password	Status of command
Help	Help information	Command	Status of command
Reboot	Reboot the module	Command and password	Status of command
Setparm	Set parameters on the module (for future use)	Command, password, parameter, and parameter value	Status of command
Status	Display troubleshooting information	Command and password	Status of command and status information
Version	Display version of module's software	Command and password	Status of command and version information

Table 3 – Local Crypto-Officer Services, Descriptions, Inputs and Outputs

Crypto-Officer Role

The Crypto-Officer role, using the Connect Server, configures and manages the module over an IPSec-secured session. Before IPSec SAs have been configured on the module, the Crypto-Officer establishes a TLS session with the module (authenticating to the module with an RSA certificate) and configures initial IPSec SAs for the Crypto-Officer over this session. The Crypto-Officer can then use IPSec-secured sessions to manage the module, including configuration of IPSec SAs on the module for both the Crypto-Officer and User roles.

The following table details the Crypto-Officer's set of services in FIPS mode.

Service	Description	Input	Output
TLS	Access the module's TLS functionality for authentication and exchange of IPSec SAs for management sessions	TLS handshake parameters, TLS inputs, IPSec SAs	TLS outputs
IPSec	Access the module's IPSec services to secure communications between the Connect Server and the module	IPSec inputs, commands, and data	IPSec outputs, status, and data.
IPSec SA configuration for Crypto-Officers	Install IPSec SAs on the module, including session keys	Command and IPSec SA information over TLS session or IPSec-secured session	Status of command over TLS session or IPSec-secured session
IPSec SA configuration for Users	Install IPSec SAs on the module, including session keys	Command and IPSec SA information over IPSec-secured session	Status of command over IPSec-secured session
IPSec SA deletion	Delete IPSec SAs on the module	Command and IPSec SA information over IPSec-secured session	Status of command over IPSec-secured session
Network configuration of the module	Configure the network settings of the module	Command and network settings over IPSec-secured session	New configuration for the module and status of command over IPSec-secured session
Base security settings configuration	Configure base security settings (HTTP, HTTPS, and DNS) on the module	Command and base security setting information over IPSec-secured session	New base security settings for the module and status of command over IPSec-secured session
Security policy configuration	Configure a security policy for the module	Command and security policy information over IPSec-secured session	Modified security policy for the module and status of command over IPSec-secured session
Security class assignment	Assign a security policy to a group of Users.	Command and assignment information over IPSec-secured session	Modified security policy for a User and Status of command over IPSec-secured session

Service	Description	Input	Output
QoS policy configuration	Configure the QoS policy of the module	Command and QoS policy information over IPSec-secured session	Modified QoS policy for the module and status of command over IPSec-secured session
Device Administration	Modify port forwarding and address translation settings on the module	Command and administration settings over IPSec-secured session	Modified administration settings for the module and status of command over IPSec-secured session
Shutdown the module	Shutdown the module	Command over IPSec-secured session	Status of command over IPSec-secured session and the module services are halted
Restart the module	Restart the module	Command over IPSec-secured session	Status of command over IPSec-secured session and the module is rebooted
Log from module	Download module logs	Initiation of IPSec-secured session	Status of command and logs over IPSec-secured session
Bypass status	Get alternating bypass status	Command over IPSec-secured session	Bypass settings of the module and status of command over IPSec-secured session

Table 4 – Crypto-Officer Services, Descriptions, Inputs and Outputs

User Role

When accessing the module's IPSec services, Users authenticate to the module per packet using the shared secret SHA-1 HMAC key provided by the Crypto-Officer as part of an IPSec SA. Additionally, Users can transfer specific packets through the module (bypass service as configured by the Crypto-Officer) without cryptographic processing. These plaintext packets are authenticated via their source and destination IP addresses and TCP ports.

The following table details the User role's set of services in FIPS mode.

Service	Description	Input	Output
IPSec	Access the module's IPSec services to secure communications between the User and the module	IPSec inputs, commands, and data	IPSec outputs, status, and data
Bypass	Transfer of specific packets between the User and the module without cryptographic processing	Plaintext data	Plaintext data and status

Table 5 – User Services, Descriptions, Inputs and Outputs

Authentication Mechanisms

The module implements password-based authentication, RSA-based authentication, and SHA-1 HMAC-based authentication mechanisms.

Authentication Type	Strength
RSA-based authentication	RSA is used by the Crypto-Officer to initially authenticate to the module using a TLS handshake. The mechanism, using a 1024-bit key size, provides a work factor of roughly 2^{80} (cryptographic strength provided by 1024-bit RSA).
SHA-1 HMAC-based authentication	The IPSec authentication mechanism of SHA-1 HMAC is used by the User and Crypto-Officer to authenticate each packet to the module. The mechanism provides a strength of 2^{96} (cryptographic strength provided by SHA-1 HMAC within IPSec).
Password-based authentication	Local Crypto-Officer passwords are required to be at least 8 characters in length and can contain all printable ASCII characters. There is a delay of 1 second after each incorrect entry of a password. Considering only the alphanumeric alphabet, the number of potential passwords is at least 62^8.
IP Address-based authentication (for bypass)	The source and destination IP addresses and TCP ports of plaintext IP packets authenticate a packet for bypass. An IP address is a 32-bit value, providing an authentication mechanism strength of at least 2^{32}.

Table 6 – Estimated Strength of Authentication Mechanisms

Unauthenticated Services

The module has unauthenticated services that do not affect any critical security parameters, and these services are available to all roles. The LEDs on the front and rear of the module provide status information. The power switch and power connector provide access to module power. The network connectors provide the ability to connect and disconnect the module from the network. Finally, the Help command on the CLI does not need an access password.

Physical Security

The Edge Controller 100x is a multi-chip standalone cryptographic module in FIPS 140-2. The EC100x is completely enclosed in a solid metal case with only specific interfaces providing access to the module. Tamper-evident labels are affixed to the module's case to provide signs of attempts to physically access the internal components of the module. (See section 3 for details on applying the tamper-evident labels.)

Cryptographic Algorithms and Protocols

The Edge Controller 100x implements the following FIPS-approved cryptographic algorithms:

- SHA-1 (Certificates #155, #156, and #157) – as per FIPS PUB 180-1
- Triple-DES (Certificates #171, #172, and #173) – as per FIPS PUB 46-3
- HMAC with SHA-1 (Certificates #155, #156, and #157, vendor affirmed) – as per FIPS PUB 198
- RSA Verification (vendor-affirmed) during TLS handshake – as per PKCS#1

The module supports the following algorithms for the following uses in a FIPS-approved mode of operation:

- Deterministic Random Number Generation – as per ANSI X9.31 (formerly ANSI X9.17)
- RSA Encryption (vendor affirmed) for key transport during TLS handshake – as per PKCS #1
- MD5 (during TLS handshake only)
- RC4-based RNG for IV generation

In addition, the EC100x supports the following protocols for use in a FIPS-approved mode of operation:

- TLSv1 – as per RFC 2246
- IPSec

Also, the module implements the following non-FIPS-approved algorithm, which is not used in a FIPS-approved mode of operation:

- HMAC - MD5

Cryptographic Key Management

The EC100x contains the following cryptographic keys and other critical security parameters (CSPs):

Key or CSP	Access by Role*	Applicable Service	Generation	Storage	Use
Shared secret Triple-DES keys for IPSec (168 bits)	Crypto-Officer – W, R, D User - R	IPSec	Outside of module (input by Crypto-Officer)	In volatile memory only (plaintext)	Encrypt and decrypt User and Crypto-Officer IPSec traffic
Shared secret SHA-1 HMAC keys for IPSec (160 bits)	Crypto-Officer – W, R, D User - R	IPSec	Outside of module (input by Crypto-Officer)	In volatile memory only (plaintext)	Authenticate User and Crypto-Officer IPSec traffic
Session keys for TLS - Triple-DES (168 bits) and HMAC (160 bits)	Crypto-Officer – W, R, D	TLS	Generated internally by module's X9.31 RNG	In volatile memory only (plaintext)	Secure TLS traffic (encrypt and MAC traffic)
Access password	Local Crypto-Officer – W, R, D	All Local CO commands except Help	N/A – chosen by Local Crypto-Officer	In non-volatile memory on disk (plaintext)	Authenticate the Local Crypto-Officer
X9.31 RNG seed and seed keys	Crypto-Officer – W, R, D	TLS	Generated internally by hardware RNG	In volatile memory only (plaintext)	Used by X9.31 RNG
Trusted CA Public keys - RSA (1024 bits or 2048 bits)	Crypto-Officer – R	TLS	Outside of module	In non-volatile memory on disk (stored in X.509 certificate)	Verify X.509 certificate to authenticate the Crypto-Officer during the TLS handshake
Policy files	Crypto-Officer – W, R, D User - R	Base Security Settings and Security Policy configuration, Device Administration, and Bypass	N/A – configured by Crypto-Officer	In non-volatile memory on disk	Bypass settings and other security policies for the module

* W – Write (input or generate) key or CSP
R – Read (use) key or CSP
D – Delete (zeroize) key or CSP

Table 7 – Description of the EC100x's Cryptographic Keys and Other CSPs

Shared secret Triple-DES keys for IPSec are ephemeral keys established for IPSec connections. These keys are loaded onto the module by the Crypto-Officer over a secure TLS connection or IPSec tunnel for Crypto-Officer sessions and over a secure IPSec tunnel for User sessions. These keys are not generated by the module. These keys are stored in volatile memory and can be destroyed by a Crypto-Officer command or by powering down the module.

Shared secret SHA-1 HMAC keys for IPSec are ephemeral keys established for IPSec connections. These keys are loaded onto the module by the Crypto-Officer over a secure TLS connection or IPSec tunnel for Crypto-Officer sessions and over a secure IPSec tunnel for User sessions. These keys are not generated by the module. These keys are stored in volatile memory and can be destroyed by a Crypto-Officer command or by powering down the module.

Session keys (3DES and SHA-1 HMAC) for the Crypto-Officer TLS session are established by the TLS handshake protocol. These keys are used to encrypt and authenticate the management session and are generated as needed by the TLS handshake. These keys are stored in volatile memory. The keys in volatile memory can be destroyed by powering down the module.

The access password is configured by the Local Crypto-Officer and is used for authenticating the Local Crypto-Officer. The password is stored on the module's hard drive. The current password can be destroyed by the Local Crypto-Officer by re-configuring the password to a new value.

The X9.31 PRNG seed and seed keys are generated by the module's hardware RNG. These keys are stored in volatile memory and can be destroyed by powering down the module.

The trusted ReefEdge CA public key certificates are loaded on the module by the manufacturer at production and are not generated by the module. These keys are used to verify the RSA certificate containing the public key of a Crypto-Officer (the Crypto-Officer role on the Connect Server authenticates to the module as the server during the TLS handshake).

The security policy files store the module's settings for bypass and other security policies (such as User security policies and QoS policies). Security policies are configured by the Crypto-Officer and are stored on the module's hard disk. The integrity of the policy files is verified at power-up and when they are modified (see Self-Tests).

Self-Tests

The Edge Controller 100x performs self-tests to monitor the proper functioning of the module. These self-tests are divided into two categories, those run during power-up and those run upon certain conditions.

Power-up Self-tests:

- Software Integrity Tests - During boot, the EC100x checks the integrity of its software using a CRC-32.
- Cryptographic Algorithm KATs - Known Answer Tests (KATs) are run at power-up for all Approved cryptographic algorithm implementations:
  - Triple-DES KAT
  - SHA-1 KAT
  - HMAC with SHA-1 KAT
  - RSA Verification KAT
  - X9.31 RNG KAT
- Statistical RNG Tests – The module performs the runs, long runs, monobit, and poker tests on its PRNG at startup.
- Startup Writable Configuration Data Integrity Check – The module checks the integrity of writable configuration data using a CRC-32.
- Bypass Mode Test -The module checks the integrity of policy files using a CRC-32.

If any integrity check fails, the module enters the bootloader error state, logs the error (if possible), and must be manually rebooted.

If any of the KATs or statistical RNG tests fail, the module enters the critical error state, logs the error, and is automatically rebooted.

Conditional Self-tests:

- Continuous Random Number Generator Test - This test is run upon generation of random data by all of the EC100x's random number generators to detect failure to a constant value.
- Bypass Mode Test - The module performs a CRC-32 check value verification to ensure that policy files have not been modified.

- Conditional Writable Configuration Data Integrity Check – The module checks the integrity of writable configuration data using a CRC-32 when the data is read or written.

If any of the conditional self-tests fail, the module enters the critical error state, logs the error, and is automatically rebooted.

Design Assurance

The development process for the Edge Controller 100x includes a configuration management (CM) system. The system in use is CVS and ReefEdge employs a branching methodology for release management. The CVS tagging mechanism is utilized to mark reproducible states in the source tree. CVS also handles all versioning of the various source code files and documentation for the EC100x.

Mitigation of Other Attacks

The module does not implement mechanisms to mitigate any other specific attacks.

SECURE OPERATION

The ReefEdge Edge Controller 100x meets Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

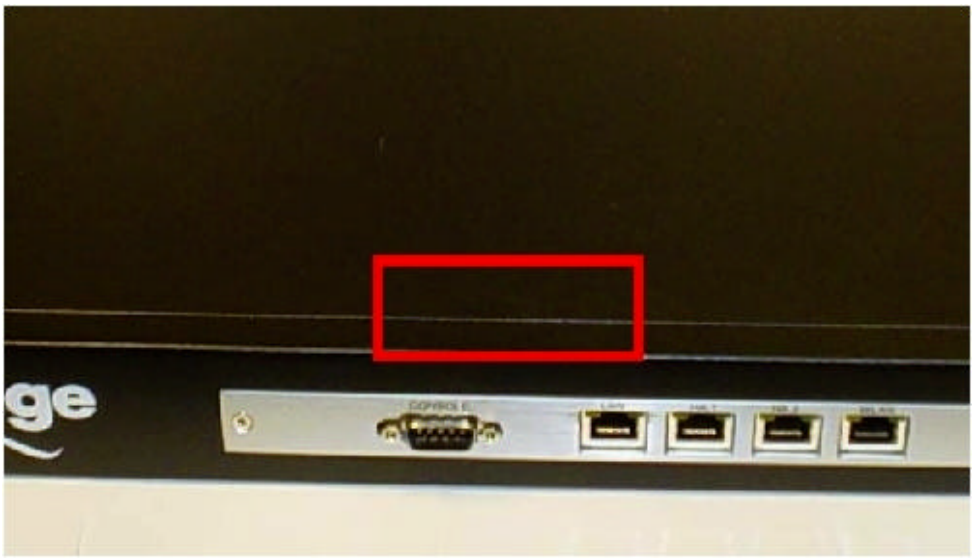
Tamper-evidence labels (shown in two of the photos below) must be applied to the module's case to provide evidence of tampering attempts. Application of the serialized tamper-evidence labels is as follows:

1. Turn off and unplug the system before cleaning the chassis and applying labels.

2. Clean the chassis of any grease, dirt, or oil before applying the tamper-evident labels. Alcohol-based cleaning pads are recommended for this purpose.

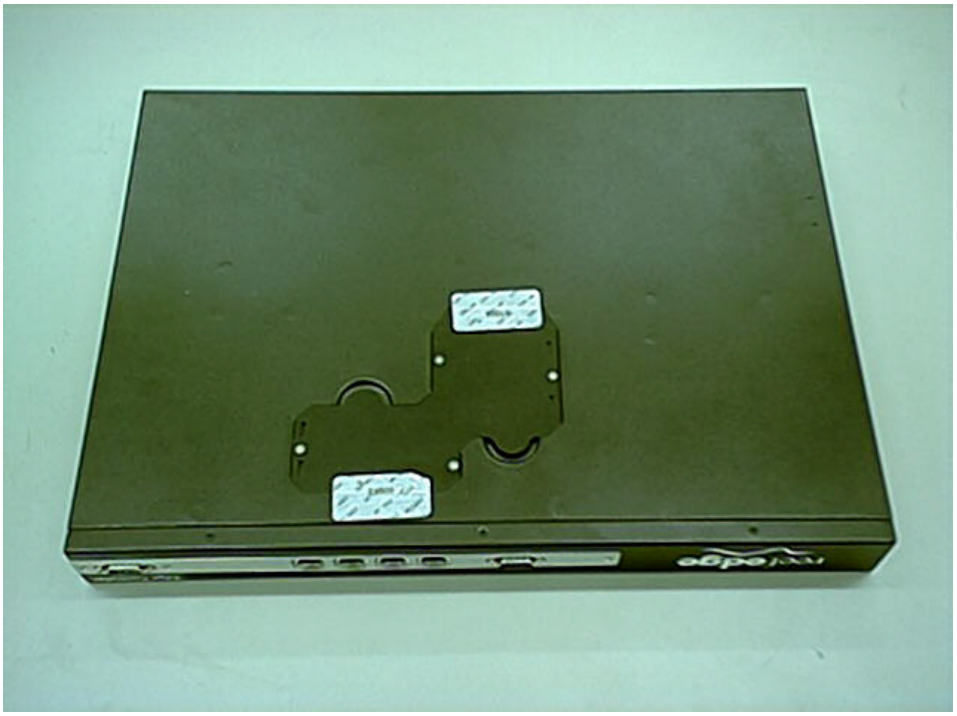
3. Apply one label over each side screw hole on the front panel.

4. Apply one label on the seam between the front and top panels.



5. Apply one label anywhere on the seam between the top cover and the rear panel (label shown in photo).

6. Apply two labels on the bottom covering the seam between the bottom of the module and the memory access door (labels shown in photo).



7. Record the serial numbers of the labels applied to the system in a security log.

8. A minimum of 12 hours is required for the labels to cure properly before the module can be used in a secure mode of operation.

The Local Crypto-Officer has to enable FIPS mode using the “Config” command via the CLI. This setting disables SSH, enables the error state for failure of the self-tests, and enforces an 8-character minimum password for the console commands. Additionally, while in the FIPS mode, the module supports FIPS-approved algorithms (SHA-1, SHA-1 HMAC, Triple-DES, and RSA-PKCS#1 Verification) and algorithms permitted for use in a FIPS mode of operation (RSA Encryption for key transport).

The Crypto-Officer has to configure IPSec and bypass services for authenticated Users. Except for specific bypass channels, wireless Users are required to use IPSec when accessing the wired network in FIPS mode.

Crypto-Officer Guidance

The Local Crypto-Officer and Crypto-Officer are responsible for initialization of the module, configuration and management of the module, and termination (shutdown) of the module. Detailed information for the Local Crypto-Officer and Crypto-Officer services can be found in the various ReefEdge Connect System manuals, including the Getting Started Guide and the Administration Guide.

Initialization

The operator(s) assuming the Local Crypto-Officer role receives the module from ReefEdge via a secure delivery mechanism. The Local Crypto-Officer can either pick the module up directly from a ReefEdge facility, or the module can be securely shipped to the Local Crypto-Officer using a bonded courier. The module is shipped in a box sealed with ReefEdge tape and is contained inside a sealed plastic bag.

If the module is shipped to the Local Crypto-Officer, the Local Crypto-Officer should examine the box and tape used to seal the box for evidence of tampering. Additionally, the Local Crypto-Officer should carefully examine the sealed bag containing the module for signs of tampering, which can include tears, scratches, and other irregularities in packaging.

Before the initial configuration of the module, there is no access control provided by the module. The Local Crypto-Officer must maintain control of the module and restrict any access to the module until configuration is

completed and the module is fully initialized for FIPS-compliant operations.

Once the EC100x is unpacked, the Local Crypto-Officer shall affix tamper-evident labels to the module's case as described above. Next, the Local Crypto-Officer must follow ReefEdge guidance for setting up the module. These steps include assuming the Local Crypto-Officer role to set the access control password for the module and configure the module's network settings.

After this process is complete, an operator can assume full Crypto-Officer responsibilities and begin managing the module via the Connect Server and can configure it for use by Users.

Management

Once the module is up and running, the Crypto-Officer role is responsible for configuration and deletion of IPSec SAs for the Crypto-Officer and Users, changing the module's settings as appropriate, and monitoring the module's status logs (as displayed on the Connect Server). The Crypto-Officer is responsible for keeping track of the module, and this includes viewing the log entries for any suspicious activities.

The Local Crypto-Officer is still required to routinely check the module's serialized, tamper-evident labels for signs of tampering. Such indications include warping, tearing, white letters appearing underneath the FIPS lettering on the top layer, and changes to the serial numbers. If strange activity or damage to labels is found, the Local Crypto-Officer should take the module offline and investigate.

If the module consistently malfunctions or otherwise repeatedly enters an error state, the manufacturer should be contacted.

Termination

When use of the EC100x has completed, the Crypto-Officer should delete all IPSec SAs, and fully power down the module to delete all remaining keys in volatile memory.

User Guidance

The User accesses the module's User services as configured by the Crypto-Officer. Although located outside the cryptographic boundary of the module, the User should be careful not to provide IPSec session keys to other parties.

ACRONYMS

ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CS	Connect Server
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
EC	Edge Controller
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
KAT	Known Answer Test
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
NDS	Novell Directory Service
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
PUB	Publication
QoS	Quality of Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SA	IPSec Security Association
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TLS	Transport Layer Security
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

