FIPS 140-2 Security Policy

CipherOptics ESG100 and CipherOptics ESG1002

Firmware Version 2.3

Hardware Versions:

ESG100, A;

ESG1002, A

ECO, Date, and Revision History
Rev A 04/07/09, Initial release
Rev B 04/30/09, Evaluation Modifications
Rev C 11/23/2009, NIST comments
Rev D 12/11/2009, NIST comments

Contact: Pam Morris
CIPHER OPTICS
701Corporate Center Drive
Raleigh, NC 27607

Checked: | Approved:

Filename: 007-004-001.pdf

Title: **FIPS 140-2 Security Policy**
CipherOptics ESG Ethernet Security Gateway

Table of Contents

Figure 1. CipherOptics ESG1002

Figure 2. CipherOptics ESG100

1 Introduction to the CipherOptics ESG Security Policy

This document describes the security policy for the CipherOptics ESG100 and ESG1002 network security appliances as required and specified in the NIST FIPS-140-2 standard. Under the standard, the CipherOptics ESG100 and ESG1002 qualify as a multi-chip stand-alone cryptographic module and satisfy overall FIPS 140-2 level 2 security requirements. In this document the CipherOptics ESG models ESG100 and ESG1002 are collectively referred to as the CipherOptics ESG.

This document applies to Firmware Version 2.3 and the following hardware versions: ESG100 version A, ESG1002 version A.

The CipherOptics ESG is in FIPS mode when the module is powered on and processing traffic using FIPS - Approved algorithms as established by the Crypto Security Officer.

This security policy is composed of:
A definition of the CipherOptics ESG's security policy, which includes:

- an overview of the CipherOptics ESG operation
- a list of security rules (physical or otherwise) imposed by the product developer

A description of the purpose of the CipherOptics ESG's security policy, which includes:

- a list of the security capabilities performed by the CipherOptics ESG

Specification of the CipherOptics ESG's Security Policy, which includes:

- a description of all roles and cryptographic services provided by the system
- a description of identification and authentication policies
- a specification of the access to security relevant data items provided to a user in each of the roles
- a description of physical security utilized by the system
- a description of attack mitigation capabilities

2 Definition of CipherOptics ESG Security Policy

2.1 CipherOptics ESG Operation Overview

The CipherOptics ESGs are high performance, integrated encryption appliances that offers full line rate Ethernet Frame encryption for 100Mbps (ESG100) and 1Gbps (ESG1002) Ethernet transports. Housed in a tamper evident chassis, the CipherOptics ESGs have two functional Ethernet ports used for traffic. The ESG100 has two

functional 10/100 Ethernet ports and the ESG1002 has two functional Gigabit Ethernet ports. Traffic on the CipherOptics ESG's local port is received from and transmitted to the trusted network in the clear, while traffic on the CipherOptics ESG's remote port has security processing applied to it. Security processing can be data confidentiality, data integrity and data authentication.

The CipherOptics ESG encrypts Ethernet Frames (Layer 2). The selection of Ethernet frame encryption is controlled by the creation and deployment of a CipherOptics ESG network security policy. From a central location, the crypto officer defines the network elements to be protected in a CipherOptics ESG policy. The policy is deployed to the CipherOptics ESG over a secure out-of-band management channel.

The CipherOptics ESG appliances can be seamlessly deployed into many network Ethernet topologies, including Metro Ethernet networks and bridged Ethernet wireless networks. The CipherOptics ESG's high-speed AES processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

The AES algorithm employed by the CipherOptics ESG appliance to encrypt/decrypt all sensitive data is the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the HMAC SHA-1 algorithm is used to provide message integrity and authentication.

Figures 3 and 4 show the physical layout of the CipherOptics ESGs. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.

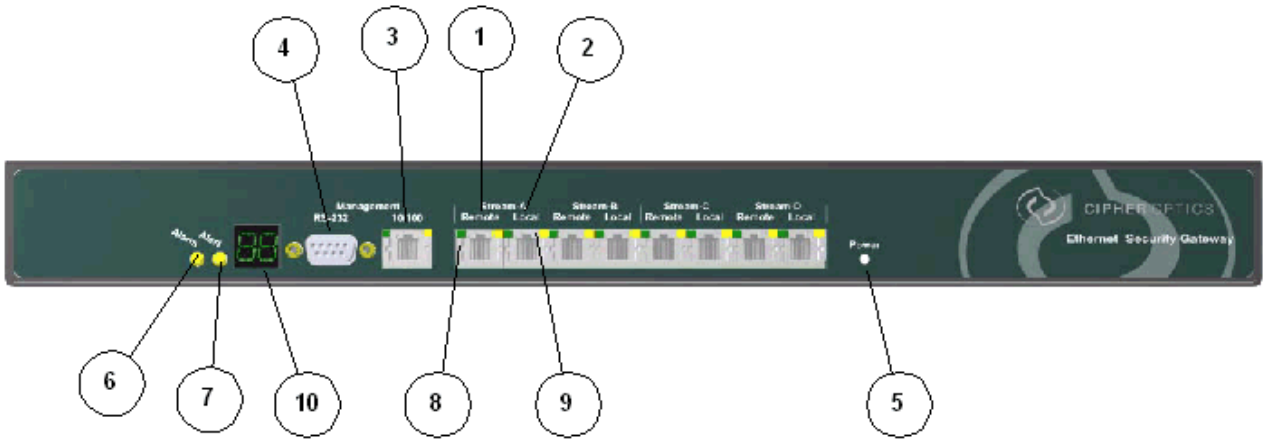

Figure 3. CipherOptics ESG100 Physical Layout of Indicators and Receptacles (Front View)

1. Remote 10/100 Ethernet Port
2. Local 10/100 Ethernet Port
3. 10/100 Ethernet Management Port
4. RS-232 Craft Port
5. Power LED
6. Alarm LED
7. Alert LED
8. Remote Port LEDs
9. Local Port LEDs
10. LCD Boot Status Indicator

Note: Only Stream A is enabled in this release of firmware. The firmware does not support the use of Streams B, C, and D. When connecting to the trusted and untrusted networks, use the Stream A local and remote ports.

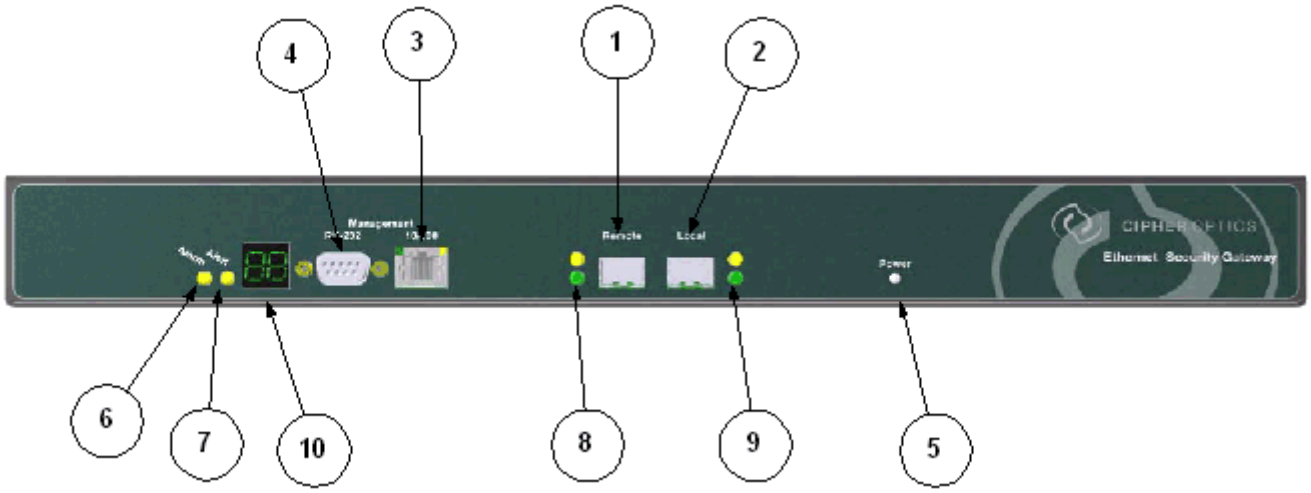

Figure 4. CipherOptics ESG1002 Physical Layout of Indicators and Receptacles (Front View)

1. Remote Gigabit Ethernet Port
2. Local Gigabit Ethernet Port
3. 10/100 Ethernet Management Port
4. RS-232 Serial Port
5. Power LED
6. Alarm LED
7. Alert LED
8. Remote Port LEDs
9. Local Port LEDs
10. LCD Boot Status Indicator

Table 1. CipherOptics ESG100 / ESG1002 Logical to Physical Port Mappings

Port	*Data Input*	*Data Output*	*Control Input*	*Status Output*
10/100 Ethernet Management Port			✓	✓
RS-232 Serial Port			✓	✓
Remote Ethernet Port	✓	✓		
Local Ethernet Port	✓	✓		

A typical operating environment is illustrated in Figure 5.

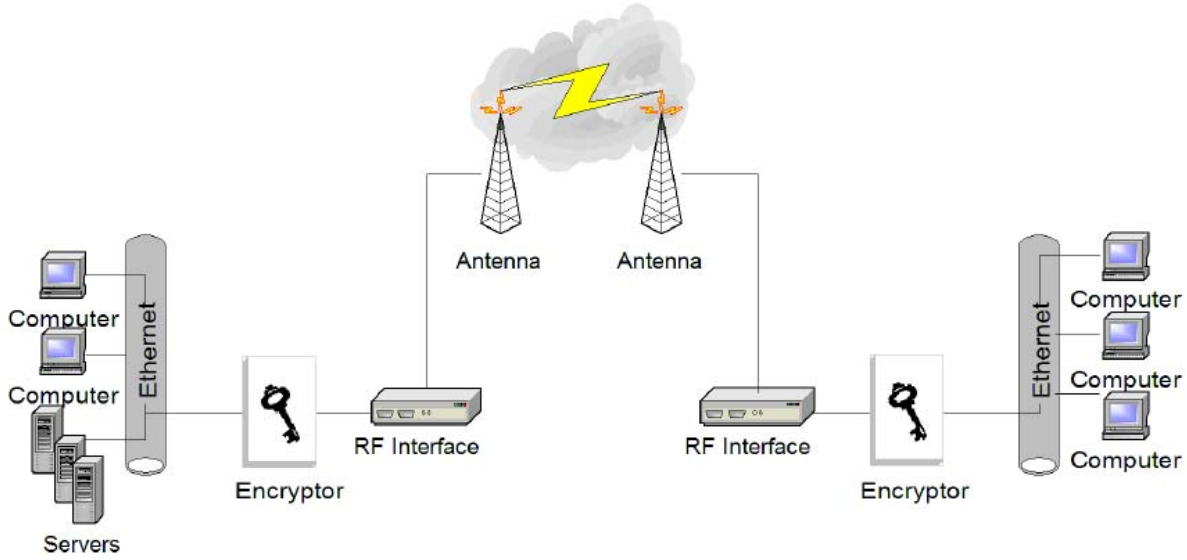

Figure 5. Typical Operational Configuration. CipherOptics ESG appliances are labeled "Encryptor."

2.2 Product Features

Hardware-based Ethernet encryption processing
Low latency
In-line network encryptor
Full duplex 200Mbps (ESG100) and 2Gbps (ESG1002) AES encryption and decryption

Comprehensive security standards support

- Encryption: AES-CBC (256 bit)
- Message Integrity: HMAC-SHA-1
- Signature Generation and Verification:
  - RSA PKCS #11
  - Random Number Generator
  - FIPS 186-2 Appendix 3.1

Table 2. Approved Security Functions

Approved Security Function	*Certificate*
Symmetric Key Encryption	
AES (CBC (e/d; 128, 192, 256))	156
TDES (TCBC (e/d; KO 1,2))	258
SHS	
SHA-1 byte-oriented	117
HMAC-SHA-1	34

Approved Security Function	*Certificate*
Asymmetric Keys	
RSA (PKCS#1) (Sig Gen and Sig Ver)	209
Random Number Generation (FIPS 186-2)	274
Non-Approved Security Function	
DES	
MD5	
HMAC MD5	
RNG-- Hardware RNG 100 used to seed the approved Random Number Generator	
Diffie-Hellman key agreement, key establishment methodology provides 90 bits of encryption strength (allowed in FIPS mode)	

Encryption
Triple-DES-CBC (168 bit)
AES (256 bit)

Message integrity
HMAC-MD5-96 (available in Non FIPS mode only)
HMAC-SHA-1

Signature Verification
RSA PKCS#1

Random Number Generation
FIPS 186-2 Appendix 3.1

CipherOptics ESG Management
Management access via the RS-232 craft port or secure 10/100 Ethernet port
Secure management access via XML-RPC (see Glossary)
Command line and web-based management interfaces
Secure IPSec session for management application
Secure telnet session for device configuration
SNMPv2c MIB managed objects supported
Alarm condition detection and reporting through audit log capability
Secure remote authenticated firmware updates

2.3 Layer 2 Ethernet Frame Encryption

The CipherOptics ESG provides encryption services to Ethernet frames, either by using a VLAN ID as an encryption selector or by encrypting all Ethernet frames received from the trusted network. The CipherOptics ESG, at Layer 2, determines which traffic to protect, how to protect it, and who to send it to. The CipherOptics ESG provides the security protocols and cryptographic keys required to provide the requested services. Because the CipherOptics ESG is encrypting and authenticating the Ethernet frame, any Layer 3 data payload can be encrypted for confidential transmission.

ESG Layer 2 security services include:
Data confidentiality - The sender can encrypt packets before sending them across a network, providing assurance that unauthorized parties cannot view the contents.
Data integrity - The receiver can authenticate packets sent by the sender to ensure that the data has not been altered in transit.
Data origin authentication -The receiver can authenticate the identity of the sender. This service is dependent on the data integrity service.

2.4 Security Rules for FIPS Level 2 Operation

The CipherOptics ESGs are bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

2.4.1 Operational Constraint

The CipherOptics ESG encryption module shall be operated in accordance with all sections of this security policy. The module shall be operated in accordance with all accompanying user documentation.

- CipherOptics ESG User Guide

2.4.2 Security Policy Limitation

This security policy is constrained to the hardware and firmware contained within the cryptographic security boundary.

2.4.3 Discretionary Access Control

Discretionary access control based roles shall be assigned in accordance with this security policy.

2.4.4 Default Deny

This module is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms shall be enabled, and the module placed in a default deny operational mode.

2.4.5 Power Requirements

It is assumed that this module is being powered at the specified line voltage (115 VAC, 60 Hertz nominal, for the United States) and that the internal DC power supply is operating normally.

2.4.6 Security Modes

The CipherOptics ESG must always be configured to FIPS-Approved encryption and message authentication – AES and SHA1.

The CipherOptics ESG GUI Interface (browser) must always operate using FIPS Approved algorithms – AES, Triple-DES, and RSA (for authentication). The browser is used for Certificate Management of the CipherOptics ESG.

The CipherOptics ESG management interface (telnet using IPSec) must always operate using FIPS-approved algorithms – AES, Triple-DES, and SHA1 authentication.

2.4.7 Physical Level Security

The CipherOptics ESG shall be installed in a controlled area with authorized personnel access only. There are tamper seals affixed to the rear of the units covering the chassis screws. The tamper seal labels are applied at the factory.

2.5 Secure Setup Procedure

The CipherOptics ESG must be set up, installed, and operated in accordance with the instructions in the User Guide.

CipherOptics ESG User Guide

For secure device management using telnet, IPSec must be enabled on the management port and a VPN Client must be installed on the management workstation. For detailed instructions refer to the CipherOptics ESG User Guide. IPSec on the management port must always operate using FIPS-approved algorithms (AES, Triple-DES encryption and SHA1 authentication). MD5 authentication is also available in non-FIPS mode operation.

The CipherOptics ESG is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms should be enabled.

The CipherOptics ESG browser interface to the Certificate Manager application must be operated using FIPS-approved algorithms (AES, or Triple-DES encryption and RSA authentication).

- Microsoft Internet Explorer version 6.0 or higher (www.microsoft.com); or
- Netscape version 7.0. (www.netscape.com)

Note: The browser must support high-grade (128-bit) security.

The CipherOptics ESG's tamper-evident seal must be intact. If the tamper-evident seal is broken, the CipherOptics ESG is not FIPS-140-2 Level 2 compliant.

The following user-supplied software must be installed on the management workstation:

- VT-100 terminal emulation utility such as HyperTerminal or TeraTerm Pro (Used to connect to the CLI through a serial link)
- Adobe Acrobat Reader version 5.0 or higher (www.adobe.com) (used to open the PDF files on the Security Gateway CD).
- VPN client application such as SafeNet High Assurance Remote

The following operating systems are supported:

- Microsoft Windows 2000
- Microsoft Windows XP
- Linux 2.4 (Red Hat Linux 7.2)

Note: The Certificate Manager application and user-supplied software are not addressed within the scope of this validation, and therefore no assurances are provided to correct operation or security.

2.6 Initiating FIPS Compliant Mode

As stated in section 2.5 (above), the CipherOptics ESG is shipped with all encryption mechanisms disabled.

To operate the CipherOptics ESG in FIPS-compliant mode the Crypto-Officer (Admin user) must:

- Log into the serial port
- Set the management IP address, subnet mask, and gateway
- Set the policy role (primary or secondary), traffic policy (clear, discard, or encrypt), and shared secret key or certificate.
- Save the configuration and policy (policy automatically reloaded)

The policy for handling data input and output will always be AES and HMAC SHA-1.

3 Purpose of a CipherOptics ESG Policy

The CipherOptics ESG is a high performance security appliance that offers Ethernet frame encryption for 100Mbps and Gigabit Ethernet (1 Gbps) traffic. The CipherOptics ESG has two Ethernet traffic ports. Traffic on the local port is received and transmitted within the trusted network in the clear, while traffic on the remote port over the internet has security processing applied to it.

The AES algorithm employed by the CipherOptics ESG to encrypt/decrypt all sensitive data is the current standard for the protection of Unclassified but Sensitive Information for the Federal Government. In addition, the HMAC SHA-1 algorithm is used to provide message integrity and authentication.

3.1 CipherOptics ESG Security Feature Overview

Key Management

Internet Key Exchange (IKE) RFCs 2408, 2409

Key Exchange

Authenticated Diffie-Hellman key exchange

Key Types

Table 3. Key Types

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Pre-Shared Key	Encryption / Decryption	32 Byte AES	Non-volatile Flash	Policy File – Plain-text
HMAC Key	Message Signing	20 Byte HMAC-SHA-1-96	Non-volatile Flash	Policy File – Plain-text
Session Encryption Key	One Symmetric Key per Security Association (SA)	32 Byte AES	Volatile SDRAM	Plain-text
Session Authentication Key	One Authentication Key per Security Association (SA)	20 Byte HMAC-SHA-1-96	Volatile SDRAM	Plain-text
Management Interface Certificate Session Key	Encrypt messages to and from policy editor	256 Bit AES 168 Bit Triple-DES	Volatile SDRAM	Plain-text
Module Keys	Authenticate messages to and from policy editor Authenticate module to remote devices	1024 Bit RSA	Non-volatile Flash	Plain-text
Firmware Upgrade Key	Authenticates firmware to be loaded	1024 Bit RSA Public	Non-volatile Flash	Plaintext
CA Root Key	Authenticates Gateway with a certificate authority	1024 or 2048 Bit RSA Public	Non-volatile Flash	Plaintext

Zeroization

Sets module to factory default keys (pre-shared key, management interface certificate session key, and module keys used to provide security during initial configuration)
Sets module to factory default policies
Sets module to factory default configurations
All plaintext keys are zeroized (volatile and non-volatile keys)

Encryption

AES-CBC (256 bit)
Triple-DES-CBC (168 bit)

Random Number Generation

FIPS 186-2 Appendix 3.1

Message Integrity

HMAC SHA-1

Signature Verification

- RSA PKCS#1

CipherOptics ESG Management
Management access via the RS-232 craft port or secure 10/100 Ethernet port
Secure management access via XML-RPC (see Glossary)
Command line and web-based management interfaces
Secure IPSec session for management application
Secure telnet session for device configuration
SNMPv2c MIB managed objects supported
Alarm condition detection and reporting through audit log capability
Secure remote authenticated firmware updates.

Role Based Access Control

Access to security configuration and device management controlled by strict userid/password authentication

3.2 Module Self-Tests

As required by FIPS 140-2, the module performs the following self-tests at start-up.

Power-Up Tests:

AES Known Answer Test
Triple-DES Known Answer Test
HMAC-SHA-1 Known Answer Test
RSA Known Answer Test
RNG Known Answer Test
Firmware Integrity Test (32 Bit CRC)
Bypass Test

Continuous Random Number Generator Test:

The module includes a continuous test on the output from the FIPS compliant RNG to FIPS 186-2. The module compares the output of the RNG with the previous output to ensure the RNG has not failed to a constant value. The Broadcom RNG 100 Random Bit Generator is a non-approved, non-deterministic hardware-based RNG. A continuous test is done for both RNGs.

Conditional Pairwise Consistency Test:

The module includes a conditional pairwise consistency test (sign and verify operation) every time RSA keys are generated.

Conditional Bypass Test:

The module includes a conditional bypass test that is performed every time a Security Policy is loaded.

Firmware Load Test:

The module includes a firmware load test with an RSA signature verification of downloaded firmware. In order for the module to maintain FIPS compliance the firmware to be upgraded must be validated to FIPS 140-2.

All data is inhibited until all the tests have completed successfully. If any of these self-tests fail, the module enters an error state and all data is inhibited. Running of the power-on self-tests is automatically initiated whenever power to the module is cycled or, on demand, by issuing the “reboot” command.

4 Specification of the CipherOptics ESG Security Policy

Three roles, that either provide security services or receive services of the Security Gateway, are the basis of the specification of the CipherOptics ESG security policy. These roles are:
Crypto Security Officer: The Crypto Security Officer role consists of the Ops user. The role defines and implements all security and network services. The role specifies the traffic to have security algorithms applied

and the transforms to be applied, defines the IP network interfaces and remote management mechanisms, and performs any firmware updates or network troubleshooting.
Crypto Security Officer A: The Crypto Security Officer "A" role consists of the Admin user. The role controls access to the CipherOptics ESG by maintaining all role-based userid/password configurations. The role specifies the traffic to have security algorithms applied and the transforms to be applied, defines the IP network interfaces and remote management mechanisms, and performs any firmware updates or network troubleshooting.
Network User: The Network User role uses the security services implemented on the Security Gateway. The Network User is any entity with an assigned IP address that matches the module's IPSec policy as defined by the Crypto Security Officer role. The CipherOptics ESG receives network user traffic on its local port. It then applies the security services to that traffic and transmits the traffic out the remote port. In addition, the CipherOptics ESG can receive encrypted traffic on its remote port, decrypt the traffic and transmit the traffic to the network user on the local port.

4.1 Identification and Authentication Policy

Login by UserID and Password, which are maintained by the Crypto Security Officer A, is the primary Identification/Authentication mechanism used to enforce access restrictions for performing or viewing security relevant events. The following table defines the Identification and Authentication Policy:

Table 4. Identification/Authentication Policy

Role	Identification/ Authentication
	CipherOptics ESG
Crypto Security Officer (CSO)	Ops UserId/Password
Crypto Security Officer A	Admin UserId/Password
Network User	Remote peer IP address and either certificate or pre-shared

Note: Any reference of CSO and CSOA under the Access Control, Roles, and Services indicates the Identification/Authentication as found in the table above.

Access of the Crypto Security Officer may be denied after unsuccessful login attempts. The Crypto Security Officer may set inactivity time outs for Login sessions.

4.2 Access Control, Roles, and Services

The roles defined above use and/or implement a number of security services in the CipherOptics ESG. Those services are:

- Test Functions – internal system test of hardware and firmware at power up or reboot
- Encryption/Decryption – services executed on Network User data
- Key Generation – services to generate and update secure key material
- Network Services – services to manage and configure the network interfaces of the system
- Security Services – services to configure and protect the security policy of the system
- Upgrade – upgrades system firmware

Table 5 defines the services, the roles that use the services, the security relevant objects created or used in the performance of the service, and the form of access given to those security relevant objects.

The cryptographic security boundary for the implementation of these services extends to the physical dimensions of a CipherOptics ESG appliance and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

Note: Items highlighted in yellow in Table 5 are Services with description of services detailed directly below highlighted area.

Table 5. Roles and Services

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Execute
CSOA	Create Passwords		
	Create or change the CSO and Admin passwords.	Password	Write, Execute
CSOA	Set Password Lockout		
	Sets how many attempts a password may be incorrectly entered.	Password	Write
CSOA	Set Password Policy		
	Sets the AR-25.2 or default password policy.	Password	Write
CSOA	Set Audit Log		
	Sets the audit-log parameters such as how many logs and were the logs will be sent.	None	Write
CSOA	View Audit Log		
	Views the audit-log information.	None	Read
CSOA	Zeroization		
	Zeroize the CipherOptics ESG.	Triple-DES, AES, RSA, Diffie-Hellman, Passwords	Execute
CSOA CSO	Run Self-Test		
	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, firmware authentication, RNG test).	None	Execute
CSOA CSO	Key Generation		
	Generate symmetric and asymmetric keys.	Triple-DES, AES, RSA, and Diffie-Hellman	Write, Execute
CSOA CSO	Configure		
	Configure IP addresses, subnets, logging, and port settings	None	Read, Write, Execute
CSOA CSO	Manage Security Policy		
	Configure Security Policy key lifetime.	Triple-DES, AES, RSA, and Diffie-Hellman	Read, Write, Execute
CSOA CSO	Show Status		
	Display network statistics, network configuration, display port information, display security policy information.	None	Read
CSOA CSO	Reboot		
	Reboot the CipherOptics ESG.	None	Execute
CSOA CSO	Edit Security Policy		
	Update the security policy rules of the CipherOptics ESG.	Triple-DES, AES, RSA	Read, Write
CSOA CSO	Firmware Upgrade		
	Update the firmware of the CipherOptics ESG.	RSA	Execute
CSOA CSO	Import/Export Key		
	Importing and exporting public keys.	RSA	Execute
Network User	Encrypt/Decrypt		
	Encrypt/Decrypt network traffic.	AES/Triple-DES session key, IPSec Session Authentication Key, CA Root Key, Diffie-Hellman	Execute

4.3 Physical Security Policy

The CipherOptics ESG system has been designed to satisfy the Level 2 physical security requirements of FIPS140-2. The system is housed in an opaque, aluminum chassis with external connections provided for the local and remote data network ports, as well as the RS-232 (serial) port, 10/100 Ethernet port, and status LEDs. The top lid and baseboard sub-assembly are attached to the case using screws. A tamper evident seal is provided over one screw in such a manner that an attempt to remove the cover requires removal of that screw and indicates subsequent evidence of tampering.

The Crypto Security Officer shall periodically check the tamper evident seal to verify that the module has not been opened. If the seal is broken, the module is no longer FIPS-140-2 compliant. The tampered module shall be returned for re-certification (following the required return procedures). Other modules, with which it exchanged keys and have no evidence of tampering, shall be zeroized.

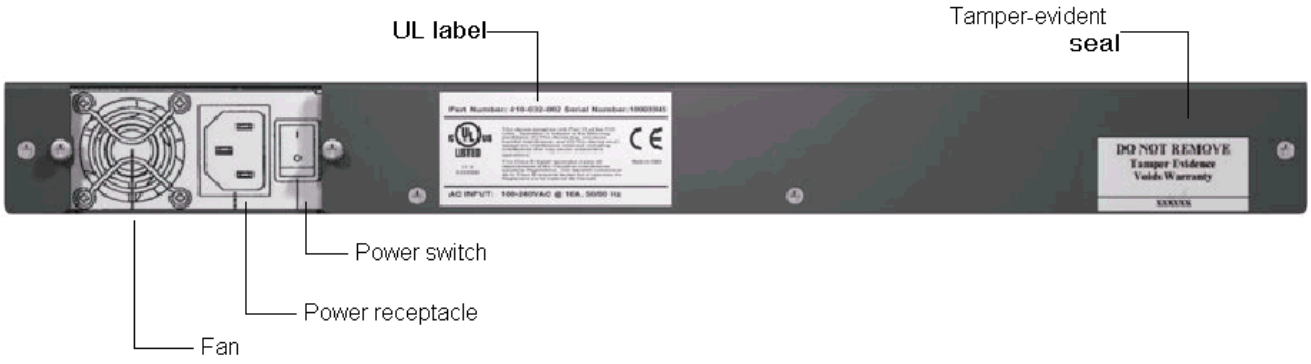

Figure 2. Rear Panel Tamper Seal, ESG100 and ESG1002

4.4 Strength of Function

Within the cryptographic security boundary, the CipherOptics ESG will only act on traffic for which a security policy has been defined. Therefore any data received for which no policy exists will be discarded. In addition, any clear traffic destined for the CipherOptics ESG's network address will be discarded. The CipherOptics ESG will only respond to IP protocol 50 and 51 and TCP/UDP port 500 packets. Thus port scans and DOS attacks are mitigated.

A secure environment relies on security mechanisms, such as firewalls, intrusion detection systems and so forth, to provide mitigation of other attacks, which could lead to a loss of integrity, availability, confidentiality, or accountability, outside of the cryptographic security boundary. Further, no mitigation is provided against clandestine electromagnetic interception and reconstruction or loss of confidentiality via covert channels (such as power supply modulation), or other techniques, not tested as part of this certification.

5 Crypto Security Officer and User Guidance

Service	Access Interface		Role Permissions		
	CLI	GUI	CSOA	CSO	Network User
Create Passwords	✓		✓		
Set Password Lockout	✓		✓		
Set Password Policy	✓		✓		
Set Audit Log	✓		✓		

Service	Access Interface		Role Permissions		
	CLI	GUI	CSOA	CSO	Network User
View Audit Log	✓		✓		
Zeroization	✓		✓		
Run Self-Test	✓		✓	✓	
Key Generation			✓	✓	
Configure	✓		✓	✓	
Create Security Policy			✓	✓	
Delete Security Policy			✓		
Show Status	✓		✓	✓	
Reboot	✓	✓	✓	✓	
Certificate Management		✓	✓	✓	
Firmware Upgrade	✓		✓	✓	
Import/Export Key			✓	✓	
Encrypt/Decrypt					✓

6 Glossary of Terms

Authentication
Authentication is the process of identification of a user, device or other entity, (typically based on a password or pass phrase) known only to a single user, which when paired with the user's identification allows access to a secure resource.

CBC
The cipher-block chaining mode of DES – See FIPS Publication 81 for a complete description of CBC mode.

Confidentiality
Confidentiality is the assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Management
Management of security features and assurances through control of changes made to hardware, firmware, or documentation, test, test fixtures, and test documentation throughout the lifecycle of the IT.

Crypto Security Officer (CSO)
The Crypto Security Officer is the individual responsible for all security protections resulting from the use of technically sound cryptographic systems. The Crypto Security Officer duties are defined within this document.

Crypto Security Officer A (CSOA)
The Crypto Security Officer A is the individual responsible for controlling access to the CipherOptics ESG by maintaining all role-base userid/password configurations. The Crypto Security Officer A duties are defined within this document.

DES
A cryptographic algorithm for the protection of Unclassified data, published in Data Encryption Standard FIPS Publication 46, DES was approved by the National Institute of Standards and Technology (NIST), and is intended for public and private use.

End to End Encryption
The totality of protection of information passed in a telecommunications system by cryptographic means, from point of origin to point of destination.

IKE
Internet Key Exchange
IP
Internet Protocol
IPSEC
Security standard for IP networks
Network User
The Network User is an ESG device that has authenticated with a remote ESG device to perform encryption/decryption services between one or more ESGs.
NIST
National Institute of Standards and Technology
Role
A Role is a pre-defined mission carrying with it a specific set of privileges and access based on required need-to-know
Role Based Access Control (RBAC)
RBAC is an access control mechanism, which restricts access to features and services used in the operation of a device based on a user's predefined mission.
Session Key
An encryption or decryption key used to encrypt/decrypt the payload of a designated packet.
Security Policy
The set of rules, regulations and laws which must be followed to ensure that the security mechanisms associated with the CipherOptics ESG are operated in a safe and effective manner. The CipherOptics ESG Security Policy shall be applied to all IP data flows through the CipherOptics ESG, per FIPS 140-2 (Level 2) requirements. It is an aggregate of public law, directives, regulations, rules, and regulates how an organization shall manage, protect, and distribute information.
TCP
Transmission Control Protocol
Tunnel
Logical IP connection in which all data packets are encrypted
UDP
User Datagram Protocol
XML-RPC
A Remote Procedure Calling protocol having a set of implementations that allow software running on disparate operating systems, running in different environments to make procedure calls over the Internet. Its remote procedure calling uses HTTP as the transport and XML as the encoding. XML-RPC is designed to be as simple as possible, while allowing complex data structures to be transmitted processed and returned.

7 References

Federal Information Processing Standard Publication 140-2 "Security Requirements for Cryptographic Modules," (Supercedes FIPS Publication 140-1, 11 January 1994
CipherOptics ESG User Guide, Version 2.3, Part Number 800-0101-001, Rev D, January 2009
CipherOptics ESG Installation Guide, Part Number 800-011-001, Rev D, January 2009
CipherOptics Security Gateway FIPS 140-2 Vendor Evidence Document, April 2004
Finite State Machine Document, November 23, 2002
Security Gateway IPSec Module Design Specification, November 27, 2002

8 Revisions

This document is an element of the Federal Information Processing Standard (FIPS) Validation process as defined in Publication 140-2. Additions, deletions, or other modifications to this document are subject to document configuration management and control. No changes shall be made once stamped FINAL, without the express approval of the Document Control Officer (DCO).

8.1 Revision History

Revision	Change Description	Change Document	Approved

A	Original Issue	CB-093	
B	Evaluation Modifications	CB-094	
C	NIST Comments	CB-095	
D	NIST Comments		