FIPS 140-2 Security Policy

CipherOptics SG100 and CipherOptics SG1002

Firmware Version 5.1

Hardware Version A

ECO, Date, and Revision History

Rev A CB-078, 05/07/04, dtm Initial release
Rev B CB084, dtm, Mods requested by Domus
Rev C CBxxx, dtm, release 3.1
Rev D CBxxx,lsr,r3.1 changes requested by Domus
Rev E, DOxxx, lsr, v3.2
Rev F, v5.1, lsr

Contact: Lynn Remaklus

Checked:

Approved:

Filename: 007-003-001f[rev5].doc

CIPHEROPTICS
701Corporate Center Drive
Raleigh, NC 27607

Title: **FIPS 140-2 Security Policy**
CipherOptics SG100 and CipherOptics SG1002

Date:	Document Number:	Rev:	Sheet:
11-30-2006	**007-003-001**	**F**	**1 of 16**

Table of Contents

Figure 1. CipherOptics SG100

Figure 2. CipherOptics SG1002

1 Introduction to the CipherOptics SG100 / SG1002 Security Policy

This document describes the security policy of the CipherOptics™ SG-series network security appliance (CipherOptics SG100 and CipherOptics SG1002) as required and specified in the NIST FIPS-140-2 standard. Under the standard, the CipherOptics SG-series system qualifies as a multi-chip stand-alone cryptographic module and satisfies overall FIPS 140-2 level 2 security requirements.

This document applies to Hardware Version A and Firmware Version 5.1.

The CipherOptics SG-series appliance is in FIPS mode when the module is powered on and processing traffic using FIPS approved cipher/authentication algorithms as established through the policy editor by the Crypto Security Officer. CipherOptics SG-series appliance and CipherOptics SGx refer to the CipherOptics SG100 and CipherOptics SG1002.

This security policy is composed of:
A definition of the CipherOptics SGx security policy, which includes:

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

A description of the purpose of the CipherOptics SGx security policy, which includes:

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

Specification of the CipherOptics SGx'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 SG-series Appliance Security Policy

2.1 CipherOptics Appliance Operation Overview

The CipherOptics SG1002 is a high performance, integrated security appliance that offers Gigabit Ethernet IPSec encryption. Housed in a tamper evident chassis, the CipherOptics SG1002 has two Gigabit Ethernet 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 CipherOptics SG100 is a high performance, integrated security appliance that offers 10/100 Ethernet IPSec encryption up to 200MB full duplex. Housed in a tamper evident chassis, the CipherOptics SG100 has two functional 10/100 Ethernet 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.

Fully compatible with existing IP networks, the CipherOptics SG-series appliance can be seamlessly deployed into Gigabit Ethernet environments, including IP site-to-site VPNs and storage over IP networks. Its high-speed AES and Triple-DES IPSec processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

Figure 3 and Figure 4 show the physical layout of the CipherOptics SG1002 and CipherOptics SG100. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.

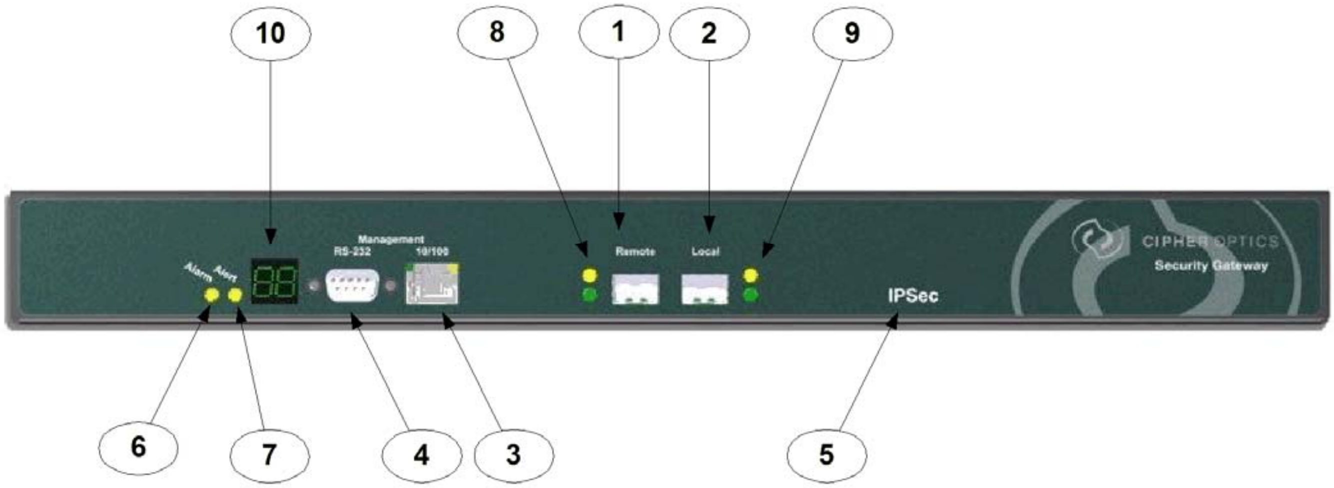

Figure 3. CipherOptics SG1002 Physical Layout of Indicators and Receptacles (Front View)

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

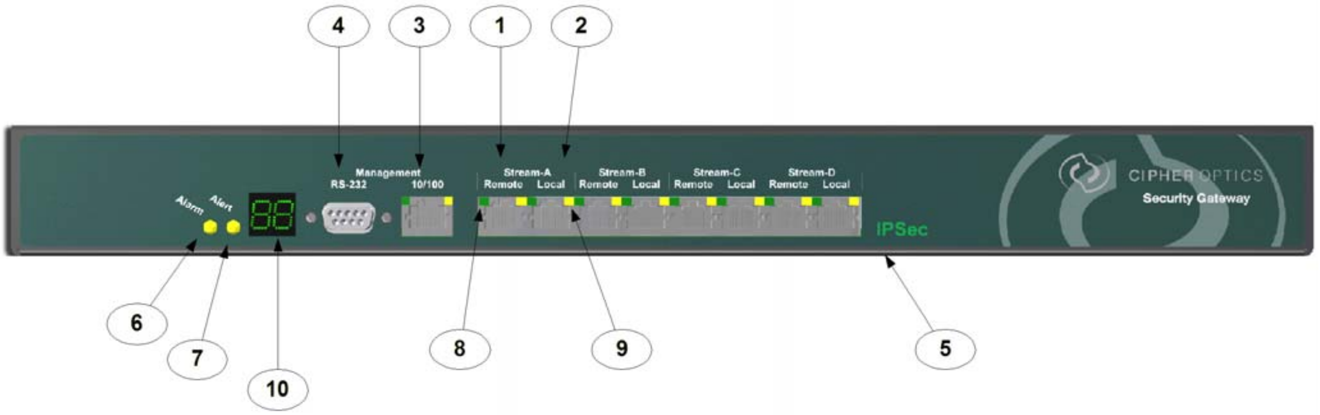

Figure 4. CipherOptics SG100 Physical Layout of Indicators and Receptacles (Front View)

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. Streams B, C, and D are not used. When connecting to the trusted and untrusted networks, use the Stream A local and remote ports.

A typical operating environment is illustrated in Figure 5.

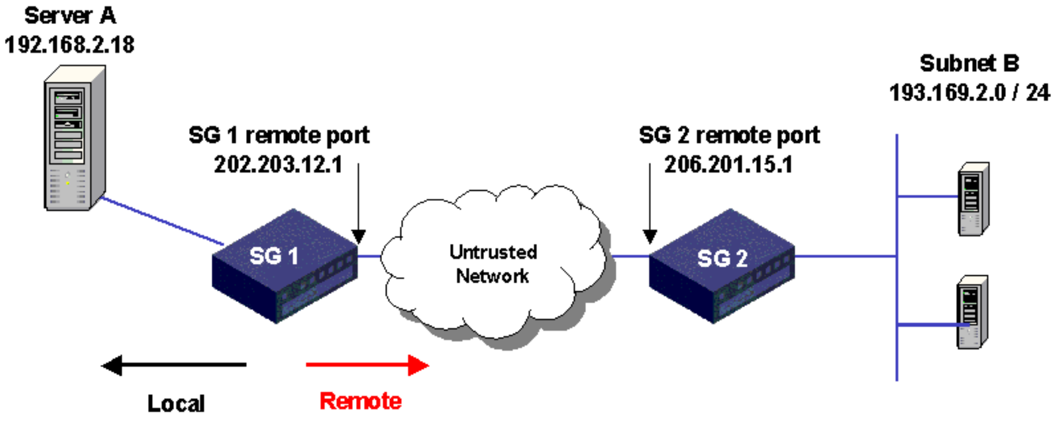

Figure 5. Typical Operational Configuration. CipherOptics appliances are labeled SG 1 and SG 2.

2.2 Product Features

Hardware-based IPSec encryption processing

- Low latency
- 1024 concurrent tunnels

Line rate Gigabit Ethernet

- CipherOptics SG1002 - Full duplex 1.8 Gbps IPSec AES and Triple-DES encryption and decryption
- CipherOptics SG100 – Full duplex 200 Mbps IPSec AES and Triple-DES encryption and decryption

Comprehensive security standards support

- Compliant with IPSec RFC 2401, 2408, 2409

- Encapsulating Security Payload (ESP) supported in Tunnel mode

Table 1. Approved Security Functions

Approved or Allowed Security Function	***Certificate***
Symmetric Key Encryption	
AES (CBC (e/d; 128, 192, 256))	156
Triple-DES (TCBC (e/d; KO 1,2,3))	258
SHS	
SHA-1 byte-oriented	117
HMAC-SHA-1	34
Asymmetric Keys	
RSA (PKCS#1) (Sig Gen and Sig Ver)	209
Random Number Generation (FIPS 186-2)	274
Diffie-Hellman (key agreement, key establishment methodology provides 90 bits of encryption strength)	
Non-Approved Security Function	
MD5	
HMAC MD5	
DES	

Encryption

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

Message integrity

- HMAC-MD5-96 (Available in non-FIPS mode only)
- HMAC-SHA-1

Signature Generation and Verification

- RSA PKCS #1

Random Number Generation

- FIPS 186-2 Appendix 3.1

Device management

- Management access via the RS-232 serial 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
- Secure SSL-TLS session for management application
- SNMPv2c MIB managed objects supported

- Alarm condition detection and reporting through audit log capability
- Secure remote authenticated software updates
- AR-25-2 password compliance support
- Radius authentication

2.3 IPSec Technology Overview

IPSec is a framework of standards developed by the Internet Engineering Task Force (IETF) that provides a method of securing sensitive information that is transmitted over an unprotected network such as the Internet.

IPSec does this by specifying which traffic to protect, how to protect it, and who to send it to. It provides a method for selecting the required security protocols, determining the algorithms to use for the services, and putting in place any cryptographic keys required to provide the requested services. Because the IP layer provides IPSec services, they can be used by any higher layer protocol.

2.3.1 IPSec Services

IPSec 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 IPSec 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.
- Anti-replay protection - The receiver can detect and reject replayed packets.

2.4 Security Rules for FIPS Level 2 Operation

The CipherOptics SG-series appliance is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

2.4.1 Operational Constraints

The CipherOptics SG-series appliance 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 SG-series User Guide
- CipherOptics SG-series Installation Guide

2.4.2 Security Policy Limitation

This security policy is constrained to the hardware, software, 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 SG-series appliance must always use FIPS approved encryption and message authentication – AES, Triple-DES, and SHA1.

The CipherOptics SGx management interface (Telnet using IPSec) must always operate using FIPS-approved cipher/authentication algorithms – AES or Triple-DES, and SHA1 authentication. DES, MD5, HMAC-MD5 must not be used in FIPS mode.

2.4.7 Physical Level Security

The CipherOptics SG-series appliance shall be installed in a controlled area with authorized personnel access only.

2.5 Secure Setup Procedure

The CipherOptics SG-series appliance must be set up, installed, and operated in accordance with the instructions in the User Guide.

- CipherOptics SG-series User Guide
- CipherOptics SG-series Installation Guide

For secure device management using Telnet for configuration and a browser for policy management, 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 SG-series User Guide. IPSec on the management port must always operate using FIPS-approved cipher and authentication algorithms (AES or Triple-DES encryption and SHA1 authentication). MD5 authentication is also available in non-FIPS mode operation.

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

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

- Microsoft Internet Explorer version 6.1 or higher (www.microsoft.com)

The CipherOptics appliance's tamper-evident seal must be intact. If the tamper-evident seal is broken, the CipherOptics SGx 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 6.0 or higher (www.adobe.com) (used to open the PDF files on the CipherOptics CD).
- VPN client application such as SafeNet High Assurance Remote

The following operating systems are supported:

- Windows 2000
- Microsoft XP
- Linux 2.4 (Red Hat Linux 8.0)

2.6 Initiating FIPS Compliant Mode

As stated in Section 2.5, the CipherOptics SG-series appliance is shipped with all encryption mechanisms disabled. You must do the following to operate the appliance in a FIPS-compliant mode.

1. Log in as the Crypto-Security Officer A and change the default passwords for both the Crypto-Security Officer A and Crypto Security Officer roles. The minimum password length must be 8 characters.
2. Set an IP Address, network mask and network gateway for the module.
3. The Crypto Security Officer must create and load a new IPSec policy to encrypt data between two subnets. The policy must include FIPS-approved algorithms.

3 Purpose of the CipherOptics SG-series Appliance Policy

The CipherOptics SG1002 is a high performance security appliance that offers IPSec encryption for Gigabit Ethernet (1 Gbps) traffic. The CipherOptics SG1002 has two Gigabit Ethernet ports. The CipherOptics SG100 is a high performance security appliance that offers IPSec encryption for 10/100 Ethernet Traffic up to 200Mbps full duplex. 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 and Triple-DES algorithms employed by the CipherOptics SG-series appliance to encrypt/decrypt all sensitive data, are 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 SG-series Appliance Security Feature Overview

Security Features

- Hardware-based IPSec encryption processing
- Comprehensive security standards support
- Compliant with IPSec RFC 2401
- Encapsulating Security Payload (ESP) supported in Tunnel mode

Key Management

- Internet Key Exchange (IKE) RFCs 2408, 2409

Key Exchange

- Authenticated Diffie-Hellman key exchange

Key Types

Table 2. Key Types

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Pre-Shared Key	Encryption / Decryption	32 Byte AES 24 Byte Triple-DES	Non-volatile Flash	Policy File – Plain-text
HMAC Key	Message Signing	20 Byte HMAC-SHA-1	Non-volatile Flash	Policy File – Plain-text
IPSec Session Encryption Key	One Symmetric Key per IPSec Security Association (SA)	32 Byte AES 24 Byte Triple-DES	Volatile SDRAM	Plain-text
IPSec Session Authentication Key	One Authentication Key per IPSec Security Association (SA)	20 Byte HMAC-SHA-1	Volatile SDRAM	Plain-text
Management Interface Session Key	Encrypt messages to and from policy editor	256 Bit AES 168 Bit Triple-DES	Volatile SDRAM	Plain-text
CipherOptics SGx Identification Certificate	Authenticate messages to and from policy editor	1024 or 2048 Bit RSA Private	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 CipherOptics SGx with a certificate authority	1024 or 2048 Bit RSA Public	Non-volatile Flash	Plaintext

Zeroization

- Sets module to factory default keys
- Sets module to factory default policies
- Sets module to factory default configurations
- All plaintext keys are zeroized

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 Generation and Verification

- RSA (PKCS#1)

Device management

- Management access via the RS-232 serial 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
- Secure SSL-TLS session for management application
- SNMPv2c MIB managed objects supported
- Alarm condition detection and reporting through audit log capability
- Secure remote authenticated software 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 CipherOptics SGx 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 RBG 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 CipherOptics SGx includes a conditional pairwise consistency test (sign and verify operation) every time RSA keys are generated.

Conditional Bypass Test:

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

Firmware Load Test:

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

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 SG-series Appliance Security Policy

Three roles, which either provide security services or receive services of the CipherOptics SG-series appliance, are the basis of the specification of the CipherOptics SGx 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 software updates or network troubleshooting.

Administrator: The Administrator role consists of the Admin user. The role controls access to the CipherOptics SGx by maintaining all role-based userid/password configurations. The role views the audit logs on the SGx. 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 software updates or network troubleshooting.

Network User: The User role uses the security services implemented on the CipherOptics SGx. The Network User is any CipherOptics SGx appliance that is authenticated with another CipherOptics SGx appliance to perform encryption and decryption services. The CipherOptics SGx receives 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 SGx can receive encrypted traffic on its remote port, decrypt the traffic and transmit the traffic to the user on the local port.

4.1 Identification and Authentication Policy

Login by UserID and Password, which are maintained by the Administrator, 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 3. Identification/Authentication Policy

Role	Identification/ Authentication
Crypto Security Officer (CSO)	Ops UserId/Password
Administrator (Admin)	Admin UserId/Password
Network User (User)	Remote peer IP address and either Certificate or Pre-Shared Key

Note: Any reference of CSO, Admin, and User 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 three unsuccessful login attempts by default. The Administrator may set inactivity time outs for login sessions. The login restrictions apply to the CSO and Admin. They are not applicable to the Network User.

4.2 Access Control, Roles, and Services

Table 4 below 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 boundary for the implementation of these services extends to the physical dimensions of a CipherOptics SGx module and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

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

Table 4. Roles and Services

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Execute
Admin	**Create Passwords**		
	Create or change the CSO and Admin passwords.	Password	Write, Execute
Admin	**Set Password Lockout**		
	Sets how many attempts a password may be incorrectly entered.	Password	Write
Admin	**Set Password Policy**		
	Sets the AR-25.2 or default password policy.	Password	Write
Admin	**Set Audit Log**		
	Sets the audit-log parameters such as how many logs and were the logs will be sent.	None	Write
Admin	**View Audit Log**		
	Views the audit-log information.	None	Read
Admin	**Zeroization**		
	Zeroize the CipherOptics SGx.	Triple-DES, AES, RSA, Diffie-Hellman, Passwords	Execute
Admin CSO	**Run Self-Test**		
	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, software authentication, RNG test).	None	Execute
Admin CSO	**Key Generation**		
	Generate symmetric and asymmetric keys.	Triple-DES, AES, RSA, and Diffie-Hellman	Write, Execute
Admin CSO	**Configure**		
	Configure IP addresses, subnets, logging, and port settings	None	Read, Write, Execute
Admin CSO	**Create Security Policy**		
	Configure Security Policy Filters, Phase 1 and Phase 2 Encryption Algorithms, set expiration of key lifetime.	Triple-DES, AES, RSA, and Diffie-Hellman	Read, Write, Execute
Admin CSO	**Delete Security Policy**		
	Deletes Security Policy	Triple-DES, AES, RSA, and Diffie-Hellman	Execute
Admin CSO	**Show Status**		
	Display network statistics, network configuration, display port information, display security policy information.	None	Read

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Execute
Admin	**Reboot**		
CSO	Reboot the CipherOptics SGx.	None	Execute
Admin	**Edit Security Policy**		
CSO	Update the security policy rules of the CipherOptics SGx.	Triple-DES, AES, RSA	Read, Write
Admin	**Load Security Policy**		
CSO	Load an updated or saved security policy into the CipherOptics SGx.	None	Execute
Admin	**Firmware Upgrade**		
CSO	Update the firmware of the CipherOptics SGx.	RSA	Execute
Admin	**Import/Export Key**		
CSO	Importing and exporting public keys.	RSA	Execute
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 SG-series appliance has been designed by CipherOptics to satisfy the Level 2 physical security requirements of FIPS140-2. The appliance is housed in an opaque, steel 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, reload the security policies and replace the tamper seal.

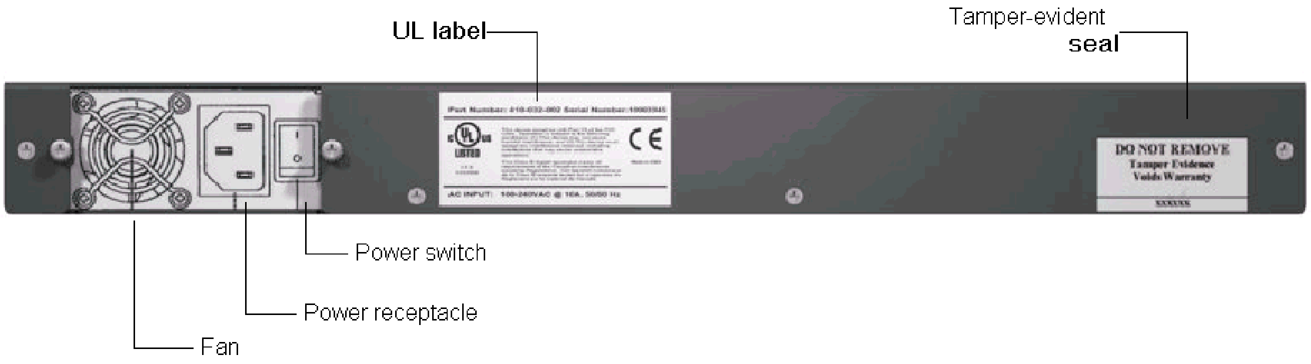

Figure 6. Rear Panel Tamper Seal, SG100 and SG1002

4.4 Strength of Function

Within the cryptographic security boundary, the CipherOptics SG-series appliance will act only 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 SGx's network address will be discarded. The appliance does not contain a bypass service. The appliance will respond only to IP protocol 50 and 51 and TCP/UDP port

500 packets. Thus port scans and DOS attacks are mitigated. To mitigate against replay attacks, an anti-replay can be enabled on the appliance.

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	Admin	CSO	User
Create Passwords	✓		✓		
Set Password Lockout	✓		✓		
Set Password Policy	✓		✓		
Set Audit Log	✓		✓		
View Audit Log	✓		✓		
Zeroization	✓		✓		
Run Self-Test	✓	✓	✓	✓	
Key Generation		✓	✓	✓	
Configure	✓		✓	✓	
Create Security Policy		✓	✓	✓	
Delete Security Policy		✓	✓	✓	
Show Status	✓		✓	✓	
Reboot	✓	✓	✓	✓	
Edit Security Policy		✓	✓	✓	
Load Security Policy	✓	✓	✓	✓	
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, software, 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 (ADMIN)

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

Network User (User)

The Network User is a CipherOptics SGx device that has authenticated with a remote CipherOptics SGx device to perform encryption/decryption services between one or more CipherOptics SGxs.

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

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 SG-series appliance are operated in a safe and effective manner. The CipherOptics SG100 and SG1002 Security Policy shall be applied to all IP data flows through the CipherOptics SGx, 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 SG-series User Guide, Version 5.1, Part Number 800-001-102, RevD, January 2007

CipherOptics SG-series Installation Guide, Part Number 800-038-003, Rev B, January 2007

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-078	05/07/04
B	Mods per NIST comments	CB-084	10/08/04
C	Version 3.1 firmware	DO-019	08/31/2005
D	Mods per NIST comments (v3.1)	DO-021	04/26/2006
E	Version 3.2 firmware	DO-xxx	8/10/2006
F	Version 5.1 firmware	DO-xxx	11/30/2006