


# FIPS 140-2 Security Policy

## cipherOptics Security Gateway

### SafeNet High Assurance 4000 Gateway

<b>ECO, Date, and Revision History</b> Rev A CB-072, 07/21/03, dtm Initial release Rev B CB-074, ttp, Mods requested by Domus	Contact: Denise McQuillin		 701 Corporate Center Drive Raleigh, NC 27607	
	Checked:	Approved:		
	Filename: 007-002-002_b2.doc			
<b>Title: FIPS 140-2 Security Policy</b> <b>cipherOptics Security Gateway SafeNet High Assurance 4000 Gateway</b>				
All rights reserved. This document may be freely copied and distributed without the Author's permission provided that it is copied and distributed in its entirety without modification.	Date: <b>1/08/04</b>	Document Number: <b>007-002-002</b>	Rev: <b>B2</b>	Sheet: <b>1 of 15</b>

**Table of Contents**

1 Introduction cipherOptics Security Gateway Security Policy ..... 3

2 Definition of Security Gateway Security Policy ..... 4

    2.1 Security Gateway Operation Overview ..... 4

    2.2 Product Features..... 5

    2.3 IPsec Technology Overview ..... 6

        2.3.1 IPsec Services..... 6

    2.4 Security Rules for FIPS Level 2 Operation ..... 6

        2.4.1 Operational Constraint..... 6

        2.4.2 Security Policy Limitation ..... 6

        2.4.3 Discretionary Access Control..... 6

        2.4.4 Default Deny ..... 6

        2.4.5 Power Requirements ..... 6

        2.4.6 Processing of Classified Information ..... 6

        2.4.7 Security Modes ..... 6

        2.4.8 Physical Level Security ..... 7

    2.5 Secure Setup Procedure..... 7

    2.6 Initiating FIPS Compliant Mode ..... 7

3 Purpose of a Security Gateway Policy ..... 8

    3.1 Security Gateway Security Feature Overview ..... 8

    3.2 Module Self-Tests ..... 9

4 Specification of the Security Gateway Security Policy ..... 9

    4.1 Identification and Authentication Policy ..... 10

    4.2 Access Control, Roles, and Services..... 10

    4.3 Physical Security Policy ..... 13

    4.4 Strength of Function..... 13

5 Glossary of Terms ..... 13

6 References ..... 15

7 Revisions ..... 15

    7.1 Revision History ..... 15



## 1 Introduction cipherOptics Security Gateway Security Policy

This document describes the security policy of the cipherOptics Security Gateway as required and specified in the NIST FIPS-140-2 standard. Under the standard, the Security Gateway system qualifies as a multi-chip stand-alone cryptographic module and satisfies overall FIPS 140-2 level 2 security requirements.

This document also applies to the SafeNet HighAssurance 4000 Gateway (HA4000). With Version 1.3 firmware the difference between the two cryptographic modules is that the HA4000 can be configured using SafeNet's SafeEnterprise Security Management Center (SMC) in addition to the CLI and GUI Policy Manager on the Module.

This document applies to Hardware Version B and C and Firmware Version 1.2.1 and Version 1.3.

The Security Gateway 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. Security Gateway refers to both cipherOptics Security Gateway and SafeNet High Assurance 4000 Gateway. Throughout this document when there are differences between the two, each will be listed separately.

This security policy is composed of:

A definition of the Security Gateway's security policy, which includes:

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

A description of the purpose of the Security Gateway's security policy, which includes:

- a list of the security capabilities performed by the Security Gateway

Specification of the Security Gateway'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

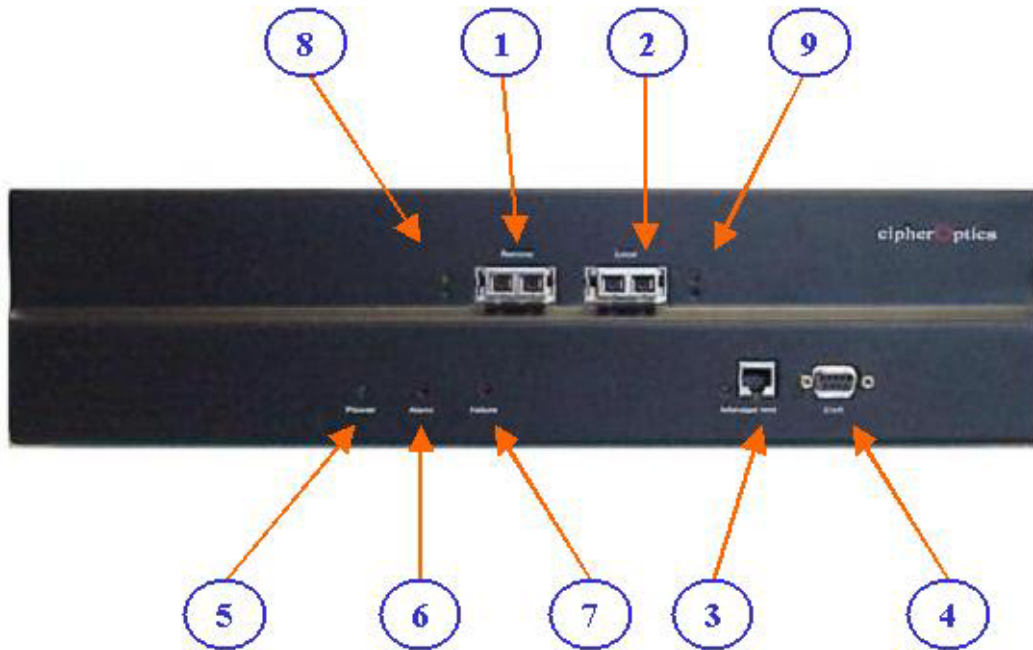
## 2 Definition of Security Gateway Security Policy

### 2.1 Security Gateway Operation Overview

The Security Gateway is a high performance, integrated security appliance that offers Gigabit Ethernet IPsec encryption. Housed in a tamper evident chassis, the Security Gateway has two Gigabit Ethernet ports. Traffic on the local port is received in the clear, while traffic on the remote port has security processing applied to it.

Fully compatible with existing IP networks, the Security Gateway can be seamlessly deployed into Gigabit Ethernet environments, including IP site-to-site VPNs and storage over IP networks. Its high-speed 3DES IPsec processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

Figure 1 shows the physical layout of the Security Gateway. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.



**Figure 1. 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 Craft Port
5. Power LED
6. Alarm LED
7. Failure LED
8. Remote Port LEDs
9. Local Port LEDs

A typical operating environment is illustrated in Figure 2.

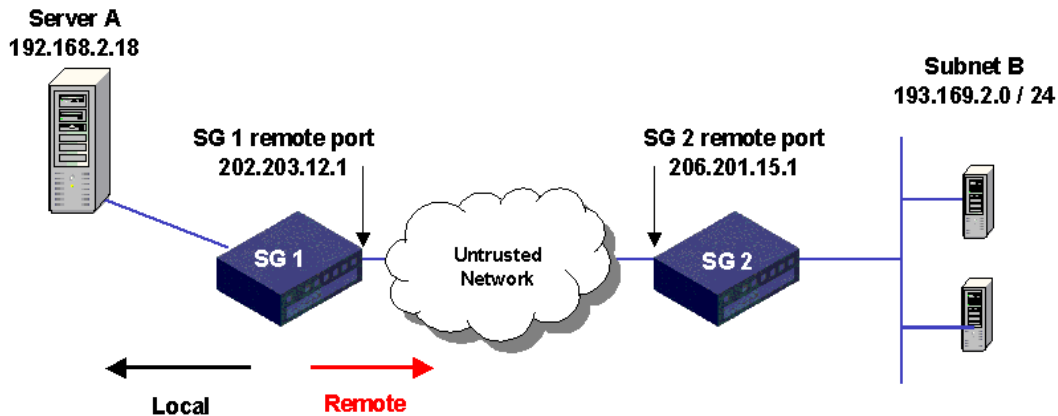


Figure 2. Typical Operational Configuration

## 2.2 Product Features

### Hardware-based IPsec encryption processing

- Low latency
- 1024 concurrent tunnels

### Line rate Gigabit Ethernet

- Full duplex 1.8 Gbps IPsec 3DES encryption and decryption

### Comprehensive security standards support

- Compliant with IPsec RFC 2401, 2408, 2409
- Encapsulating Security Payload (ESP) and Authentication Header (AH) supported in Tunnel mode

### Encryption

- DES-CBC (56 bit) [ for legacy support only ]
- 3DES-CBC (168 bit)

### Message integrity

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

### Signature Verification

- RSA (PKCS#1, Vendor Affirmed)

### Device management cipherOptics Security Gateway and SafeNet HighAssurance 4000 Gateway

- 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 SSL 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 software updates

### Additional Device management SafeNet HighAssurance 4000 Gateway

- Secure management access via SafeEnterprise Security Management Center (SMC)
- SMC and device use of XML-RPC

## 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 Security Gateway is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

### 2.4.1 Operational Constraint

The Security Gateway 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 Security Gateway User Guide, Release 1.3
- SafeNet HighAssurance 4000 Gateway User's 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 Processing of Classified Information

This module shall not process, protect, or store classified information.

### 2.4.7 Security Modes

The Security Gateway must always be configured to FIPS approved encryption and message authentication – 3DES/DES and SHA1.

The Security Gateway GUI Interface (browser) must always operate using FIPS approved cipher/authentication algorithms - 3DES/DES and RSA (for authentication). The browser is used for Policy Management of the Security Gateway.

The Security Gateway management interface (telnet using IPSec) must always operate using FIPS-approved cipher/authentication algorithms -DES, 3DES, and SHA1 authentication.

### 2.4.8 Physical Level Security

The Security Gateway shall be installed in a controlled area with authorized personnel access only.

### 2.5 Secure Setup Procedure

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

- cipherOptics Security Gateway User Guide, Release 1.3
- SafeNet HighAssurance 4000 Gateway User's 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 Security Gateway User Guide, Release 1.3. IPSec on the management port must always operate using FIPS-approved cipher and authentication algorithms (DES, 3DES encryption and SHA1 authentication). MD5 authentication is also available in non-FIPS mode operation.

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

- The Security Gateway browser interface to the Policy Manager application must be operated using FIPS-approved cipher and authentication algorithms (DES or 3DES encryption and RSA authentication).
  - Microsoft Internet Explorer version 6.0 or higher ([www.microsoft.com](http://www.microsoft.com)); or
  - Netscape version 7.0. ([www.netscape.com](http://www.netscape.com))

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

The Security Gateway's tamper-evident seal must be intact. If the tamper-evident seal is broken, the Security Gateway 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](http://www.adobe.com)) (used to open the PDF files on the Security Gateway CD).
- VPN client application such as SSH Sentinel
- If using the SafeNet HA4000, the SafeEnterprise Security Management Center may also be installed to manage the module. The SafeEnterprise Security Management Center User's Guide must be used to install the SMC application.

The following operating systems are supported:

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

### 2.6 Initiating FIPS Compliant Mode

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

For the cipherOptics Security Gateway to initiate the module in FIPS Compliant mode the Crypto-Officer (Ops User) must create and load a policy (via the Policy Editor) that uses DES or 3DES for data encryption and HMAC SHA-1 for authentication.

For the SafeNet HighAssurance 4000 Gateway to initiate the module in FIPS Compliant mode the Crypto-Officer (Admin User) must create and load a policy (via the Policy Editor) that uses DES or 3DES for data encryption and HMAC SHA-1 for authentication or use SMC to configure the module and create a policy.

**NOTE:** MD5 is not a FIPS-approved authentication algorithm. Using MD5 authentication in a security policy takes the Security Gateway out of FIPS compliant operation.

### 3 Purpose of a Security Gateway Policy

The Security Gateway is a high performance security appliance that offers IPSec encryption for Gigabit Ethernet (1 Gbps) traffic. The Security Gateway has two Gigabit Ethernet ports. Traffic on the local port is received and transmitted in the clear, while traffic on the remote port has security processing applied to it.

The 3DES algorithm employed by the Security Gateway to encrypt/decrypt all sensitive data, is the current de-facto standard for the protection of Unclassified and Sensitive Unclassified Information for the Federal Government. In addition, the SHA-1 algorithm is used to provide message integrity and authentication.

#### 3.1 Security Gateway Security Feature Overview

##### Security Features

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

##### Key Management

- Internet Key Exchange (IKE) RFCs 2408, 2409

##### Key Exchange

- Authenticated Diffie-Hellman key exchange

##### Key Types

Key Name	Description and /or Purpose	Type of Key	Storage Location	Storage Method
Manual Key Cipher Secret	Encryption / Decryption	24 Byte 3DES 8 Byte DES	Non-volatile Flash	Policy File – Plain-text
Manual Key Hash Secret	Message Signing	20 Byte HMAC-SHA-1-96	Non-volatile Flash	Policy File – Plain-text
IPSec Session Encryption Key	One Symmetric Key per IPSec Security Association (SA)	24 Byte 3DES	Volatile SDRAM	Plain-text
IPSec Session Authentication Key	One Authentication Key per IPSec 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	168 Bit 3DES	Volatile SDRAM	Plain-text
Management Interface Certificate Private Key	Authenticate messages to and from policy editor	1024 Bit RSA	Non-volatile Flash	Plain-text

##### 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



- 3DES-CBC (168 bit)
- DES-CBC (56 bit) [ for legacy support only ]

**Message integrity**

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

**Signature Verification**

- RSA (PKCS#1, Vendor Affirmed)

**Device management cipherOptics Security Gateway and SafeNet HighAssurance 4000 Gateway**

- 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 SSL 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 software updates using a CRC. Note: Firmware updates will be done at the factory.

**Additional Device management SafeNet HighAssurance 4000 Gateway**

- Secure management access via SafeEnterprise Security Management Center (SMC)
- SMC and device use of XML-RPC

**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:**

- 3DES Known Answer Test
- DES Known Answer Test
- HMAC-SHA-1 Known Answer Test
- Pair wise consistency test for RSA and Diffie-Hellman
- Software Integrity Test

**Continuous Random Number Generator Test:**

- The module includes a continuous test on the output from the FIPS compliant RNG. The module compares the output of the RNG with the previous output to ensure the RNG has not failed to a constant value.

If any of these self-tests fail, the module enters an error state.

- All data is inhibited during self-tests. Running of the above tests is automatically initiated whenever power to the module is cycled or, on demand, by issuing the “reboot” command.

**4 Specification of the Security Gateway Security Policy**

Three roles, that either provide security services or receive services of the Security Gateway, are the basis of the specification of the Security Gateway security policy. These roles are:

- **Crypto Security Officer:** The Crypto Security Officer role consists of the Ops user on the cipherOptics Security Gateway and the Admin user on the SafeNet HighAssurance 4000 Gateway. 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.

- **Crypto Security Officer A:** The Crypto Security Officer “A” role consists of the Admin user on the cipherOptics Security Gateway and the Super user on the SafeNet HighAssurance 4000 Gateway. The role controls access to the Security Gateway by maintaining all role-based userid/password configurations.
- **User:** The User role uses the security services implemented on the Security Gateway. The User is any entity with an assigned IP address that matches the module’s IPSec policy as defined by the Crypto Security Officer User role. The Security Gateway 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 Security Gateway 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 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:

Role	Identification/ Authentication	
	CipherOptics Security Gateway	SafeNet HighAssurance 4000 Gateway
Crypto Security Officer (CSO)	Ops UserId/Password	Admin UserId/Password
Crypto Security Officer A (CSOA)	Admin UserId/Password	Super UserId/Password
User	IPSec Policy	IPSec Policy

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

**Table 1 - Identification/Authentication Policy**

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 Security Gateway. Those services are:

- Test Functions – internal system test of hardware and software at power up or reboot
- Encryption/Decryption – services executed on 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 software

Table 2 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 Security Gateway module and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

Note: Items highlighted in blue in Table 2 are Services with description of services detailed directly below highlighted area.

**Table 2 - Roles and Services**

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Edit, Delete, Use
<b>Self-Test Functions Service</b>			
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> Reboot command initiated via CLI or Web Browser <i>SafeNet HA4000 Gateway</i> Reboot command initiated via SMC <b>CSOA:</b> Reboot command initiated via CLI only	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, software authentication, RNG test).	Encrypt/decrypt test of algorithms	Use
<b>Encryption/Decryption Service</b>			
<b>User</b>	<b><u>Transparent to User:</u></b> <ul style="list-style-type: none"> <li>• Receive/Generate IP Packets</li> <li>• User or server creates packet and transmits to system</li> <li>• Clear packets (i.e. plain text) are presented to the input local network port for encryption. Encrypted packet is output on remote network port.</li> </ul>	/3DES Session Key	Write
<b>Key Generation Service</b>			
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> Login to the policy editor via the secure web browser <i>SafeNet HA4000 Gateway</i> Login to SMC policy editor	IKE policy definition	Diffie-Hellman	Write/Edit
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> Login to the policy editor via the secure web browser <i>SafeNet HA4000 Gateway</i> Login to SMC policy editor	For IKE negotiated policy: The CSO enters the pre-shared secret <b>Note: <i>the pre-shared secret is used by the module in the generation of the Encryption/Decryption Keys.</i></b>  For manual key policy <sup>1</sup> : The CSO enters the Encryption/Decryption Key  <b>Note: <i>The CSO sets the lifetime of the Cipher keys for an IKE negotiated policy (once the lifetime expires, new keys are automatically generated by the module).</i></b>	3DES Session Key  Diffie-Hellman	Write/Use
<p><sup>1</sup> The Security Gateway's "Manual Key Policy" is a form of <b>Electronic Key Entry</b> and should not be confused with "Manual Key Entry", as defined by the FIPS 140-2 Standard. The Ops User, after entering the Policy Editor via the secure web browser connection and creating a new Manual Key Policy, manually types into the GUI interface 48 HEX values (which equals 192 bits). When the new Manual Key Policy is saved and loaded, the 48 HEX values are sent to the module via the secure web browser connection and the module's internal mechanism uses these bits to create the 3DES keys.</p> <p>Note: SMC is not capable of creating a Manual Key Policy (although the SafeNet HA 4000 Gateway can still create a Manual key Policy via the Policy Editor by authenticating to the module via the Secure Web Browser).</p>			
<b>Network Services</b>			

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Edit, Delete, Use
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway via CLI only</i> <i>SafeNet HA4000 Gateway In addition via SMC*</i>	Specification of remote/ local network addresses*	Network Data	Write/Use
	Specification of management address*	Network Data	Write/Use
	Specification of SNMP attributes	Network Data	Write/Use
	Show status • Display network statistics	Data	Read
	Show configuration • Display network configuration	Data	Read
<b>Security Services</b>			
<b>CSOA:</b> via CLI	Define and maintain userids and passwords	Userid/ Passwords	Write/Edit/Use
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> Defined in policies using Policy Editor via secure web browser <i>SafeNet HA4000 Gateway</i> Defined in policies using Policy Editor via SMC	Define security policies for encryption/discard	Desired filters	Write/Edit
<b>CSO:</b> via CLI	Show status • Display security status of each established channel/path - Terminal output also indicates error status • Show Configuration • Display current network and security configuration.	Data	Read
<b>CSO:</b> via CLI (command "Clear All")	System Zeroization  Manual Keys All pre-shared secrets Diffie-Hellman Keys IPSec Session Keys (DES, 3DES)	Cryptographic Key data  Policies  Configurations	Delete/Write  Delete/Write  Delete/Write  <b>Note: During zeroization, the factory default keys, polices &amp; configurations overwrite the current information on the module.</b>
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> via secure web browser <i>SafeNet HA4000 Gateway</i> via SMC	Expiration of key lifetime <b>Note: The CSO sets the lifetime of the Cipher keys for an IKE negotiated policy (once the lifetime expires, new keys are automatically generated by the module).</b>	Encryption Key  DES/3DES	Delete/Write
<b>CSO:</b> <i>CipherOptics Security Gateway and</i>	System reboot	Clear IKE negotiated keys	Read/Delete

Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Edit, Delete, Use
<i>SafeNet HA4000 Gateway</i> via CLI and secure web browser <i>SafeNet HA4000 Gateway</i> via SMC <b>CSOA:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> via CLI	Policy Reload		
<b>Upgrade</b>			
<b>CSO:</b> <i>CipherOptics Security Gateway and SafeNet HA4000 Gateway</i> via CLI <i>SafeNet HA4000 Gateway</i> via SMC	New software downloaded to system [software updates are not allowed in FIPS mode]	Firmware updates will be done at the factory.	Write/Use

### 4.3 Physical Security Policy

The Security Gateway system has been designed by cipherOptics to satisfy the Level 2 physical security requirements of FIPS140-2. The system is housed in an opaque, steel chassis with external connections provided for the local and remote data network ports, as well as the Craft (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 to cipherOptics for re-certification (following the required return procedures). Other modules with which it exchanged keys and have no evidence of tampering, shall be zeroized.

### 4.4 Strength of Function

Within the cryptographic security boundary, the Security Gateway 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 Security Gateway's network address will be discarded. The Security Gateway 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 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 (CSOA)**

The Crypto Security Officer A is the individual responsible for controlling access to the Security Gateway 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

### **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 Security Gateway are operated in a safe and effective manner. The cipherOptics Security Gateway Security Policy shall be applied to all IP data flows through the Security Gateway, 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. It's 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.

## 6 References

Federal Information Processing Standard Publication 140-2 "Security Requirements for Cryptographic Modules," (Supercedes FIPS Publication 140-1, 11 January 1994)

Public law 100-235, "Computer Security Act of 1987" 8 January, 1988

Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," 8 February 1996

Director of Central Intelligence 1/16, "Security Policy on Intelligence Information in Automated Systems and Networks," 14 March 1988

Trusted Network Interpretation , Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005, Version 1, 31 July 1987)

Department of Defense Standard, (DoD Trusted Computer System Evaluation Criteria, 1987 5200.28-STD, December 1985

Common Criteria, (Common Criteria Implementation Board (CCIB) International Standard 15408, Common Criteria for Information Technology Security Evaluation) Version 2, May 1998, ISO/IEC JTC 1 and Common Criteria Implementation Board

National Institute of Standards and, Computer Data Authentication, Federal Information Processing Standards Publication 113, 30 May 1985

DoDI 2200.40 Defense Information Technology Certification and Accreditation Process (DITSCAP) 30 December 1997

cipherOptics Security Gateway Release 1.1 User Guide, Part Number 800-001-002, November 2002

## 7 Revisions

This document is an element of the Federal Information Processing Standard (FIPS) Certification 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).

### 7.1 Revision History

Revision	Change Description	Change Document	Approved
A	Original Issue	CB-072	07/21/03
B	Mods per NIST comments	CB-074	12/17/03