FIPS 140-2 Security Policy

SafeNet HighAssurance 4000 Gateway

Firmware Version 5.1

Hardware Version A

ECO, Date, and Revision History
Rev A CB-078, 05/07/04, dtm Initial release
Rev B CB-084,dtm, Mods requested by Domus
Rev C CB-xxx, lsr, new firmware version
Updated Firmware Revision

Contact: Scott Palmquist

Checked:

Approved:

Filename: 007-002-101_d(1)-SafeNet.doc

4690 Millennium Drive, Suite 400
Belcamp, Maryland 21017

Title: **FIPS 140-2 Security Policy**
SafeNet HighAssurance 4000 Gateway

Date:	Document Number:	Rev:	Sheet:
07/09/2008	**007-002-101**	**D**	**1 of 16**

Table of Contents

1 Introduction SafeNet HighAssurance 4000 Gateway Security Policy

This document describes the security policy of the SafeNet HighAssurance 4000 Gateway as required and specified in the NIST FIPS-140-2 standard. Under the standard, the HighAssurance 4000 Gateway 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 HighAssurance 4000 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.

This security policy is composed of:
A definition of the HighAssurance 4000 Gateway's security policy, which includes:

- an overview of the HighAssurance 4000 Gateway operation
- a list of security rules (physical or otherwise) imposed by the product developer

A description of the purpose of the HighAssurance 4000 Gateway's security policy, which includes:

- a list of the security capabilities performed by the HighAssurance 4000 Gateway

Specification of the HighAssurance 4000 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 HighAssurance 4000 Gateway Security Policy

2.1 HighAssurance 4000 Gateway Operation Overview

The HighAssurance 4000 Gateway is a high performance, integrated security appliance that offers Gigabit Ethernet IPSec encryption. Housed in a tamper evident chassis, the HighAssurance 4000 Gateway 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.

Fully compatible with existing IP networks, the HighAssurance 4000 Gateway can be seamlessly deployed into Gigabit Ethernet environments, including IP site-to-site VPNs and storage over IP networks. Its high-speed AES and 3DES IPSec processing eliminates bottlenecks while providing data authentication, confidentiality, and integrity.

Figure 1 shows the physical layout of the HighAssurance 4000 Gateway. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.

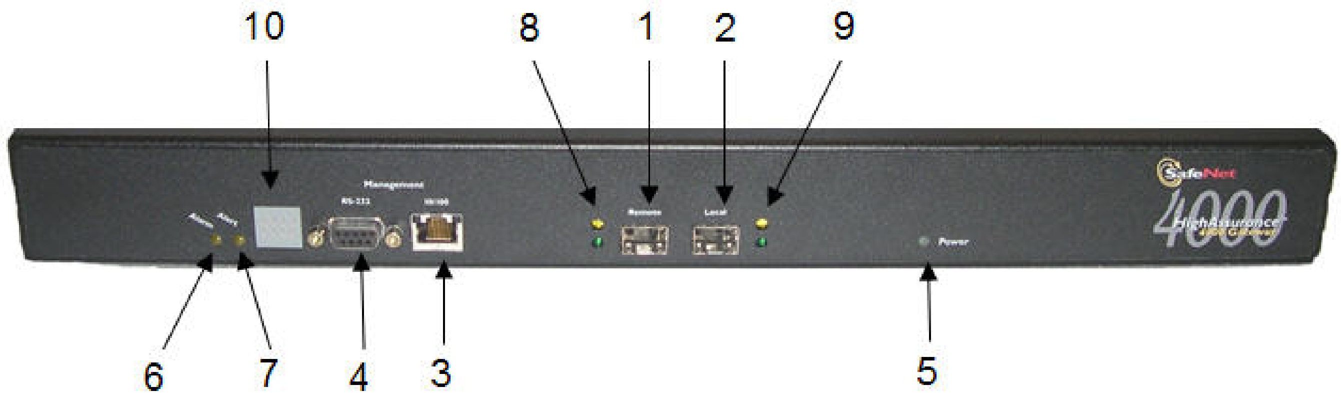

Figure 1. Physical Layout of Indicators, and Receptacles (Front View)

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
10. LCD Boot Status Indicator

A typical operating environment is illustrated in Figure 2.

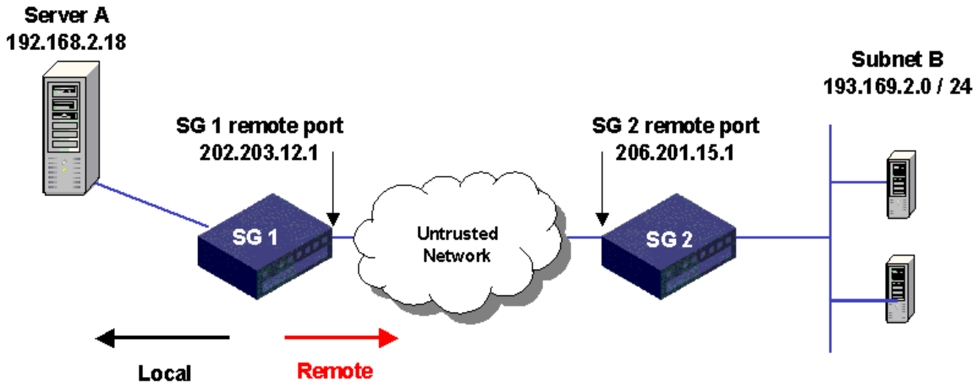

Figure 2. Typical Operational Configuration

2.2 Product Features

Hardware-based IPSec encryption processing

- Low latency
- 10,000 concurrent tunnels

Line rate Gigabit Ethernet

- Full duplex 1.8 Gbps IPSec AES and 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

Approved Security Function	*Certificate*
Symmetric Key Encryption	
AES (CBC (e/d; 128, 192, 256))	156
TDES (TCBC (e/d; KO 1,2,3))	258
DES (CBC (e/d (for legacy systems only))	260
SHS	
SHA-1 byte-oriented	117
HMAC-SHA-1 (vendor affirmed)	34
Asymmetric Keys	
RSA (PKCS#1) (Sig Gen and Sig Ver) (vendor affirmed)	209
Random Number Generation (FIPS 186-2)	274
Non-Approved Security Function	
DES	
MD5	

Approved Security Function	*Certificate*
HMAC MD5	

Encryption

- 3DES-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

Device management 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 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 software updates
- Secure management access via SafeEnterprise Security Management Center (SMC)
- SMC and device use of XML-RPC
- 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 HighAssurance 4000 Gateway is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

2.4.1 Operational Constraint

The HighAssurance 4000 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.

- 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 Security Modes

The HighAssurance 4000 Gateway must always be configured to FIPS approved encryption and message authentication – AES, 3DES, and SHA1.

The HighAssurance 4000 Gateway GUI Interface (browser) must always operate using FIPS approved cipher/authentication algorithms – AES, 3DES, and RSA (for authentication). The browser is used for Policy Management of the HighAssurance 4000 Gateway.

The HighAssurance 4000 Gateway management interface (telnet using IPSec) must always operate using FIPS-approved cipher/authentication algorithms – AES, 3DES, and SHA1 authentication.

2.4.7 Physical Level Security

The HighAssurance 4000 Gateway shall be installed in a controlled area with authorized personnel access only.

2.5 Secure Setup Procedure

The Security HighAssurance 4000 Gateway must be set up, installed, and operated in accordance with the instructions in the User Guide.

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

The HighAssurance 4000 Gateway is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms should be enabled.

- The HighAssurance 4000 Gateway browser interface to the Policy Manager application must be operated using FIPS-approved cipher and authentication algorithms (Astor 3DES 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 HighAssurance 4000 Gateway's tamper-evident seal must be intact. If the tamper-evident seal is broken, the HighAssurance 4000 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) (used to open the PDF files on the Security Gateway CD).
- VPN client application such as SSH Sentinel
- 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 HighAssurance 4000 Gateway is shipped with all encryption mechanisms disabled.

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 AES 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 HighAssurance 4000 Gateway Policy

The HighAssurance 4000 Gateway is a high performance security appliance that offers IPSec encryption for Gigabit Ethernet (1 Gbps) traffic. The HighAssurance 4000 Gateway 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 AES and 3DES algorithm employed by the HighAssurance 4000 Gateway 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 HighAssurance 4000 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

Pre-Shared Key	Encryption / Decryption	32 Byte AES 24 Byte 3DES 8 Byte DES	Non-volatile Flash	Policy File – Plain-text
HMAC Key	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)	32 Byte AES 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	256 Bit AES 168 Bit 3DES	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-Volitle 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
- Sets module to factory default policies
- Sets module to factory default configurations
- All plaintext keys are zeroized

Encryption

- AES-CBC (256 bit)
- 3DES-CBC (168 bit)

Random Number Generation

- FIPS 186-2 Appendix 3.1

Message integrity

- HMAC SHA-1

Signature Verification

- RSA PKCS#1

Device management 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 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 software updates.
- 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:

- AES Known Answer Test
- 3DES 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 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 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 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 HighAssurance 4000 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 HighAssurance 4000 Gateway security policy. These roles are:

- Crypto Security Officer: The Crypto Security Officer role consists of the Admin 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.
- Crypto Security Officer A: The Crypto Security Officer “A” role consists of the Super user. The role controls access to the HighAssurance 4000 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 HighAssurance 4000 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 HighAssurance 4000 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**
	SafeNet HighAssurance 4000 Gateway
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.

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 HighAssurance 4000 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 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 High Assurance 4000 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, 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 HA4000.	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, software 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**	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
CSOA **CSO**	Delete Security Policy		
	Deletes Security Policy	Triple-DES, AES, RSA, and Diffie-Hellman	Execute
CSOA **CSO**	Show Status		
	Display network statistics, network configuration, display port information, display security policy information.	None	Read
CSOA **CSO**	Reboot		
	Reboot the HA4000	None	Execute
CSOA **CSO**	Edit Security Policy		
	Update the security policy rules of the HA4000.	Triple-DES, AES, RSA	Read, Write
CSOA	Load Security Policy		

CSO			
	Load an updated or saved security policy into the HA4000.	None	Execute
CSOA **CSO**	Firmware Upgrade		
	Update the firmware of the HA4000.	RSA	Execute
CSOA **CSO**	Import/Export Key		
	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 HighAssurance 4000 Gateway system has been designed 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 for re-certification (following the required return procedures). Other modules with which it exchanged keys and have no evidence of tampering, shall be zeroized.

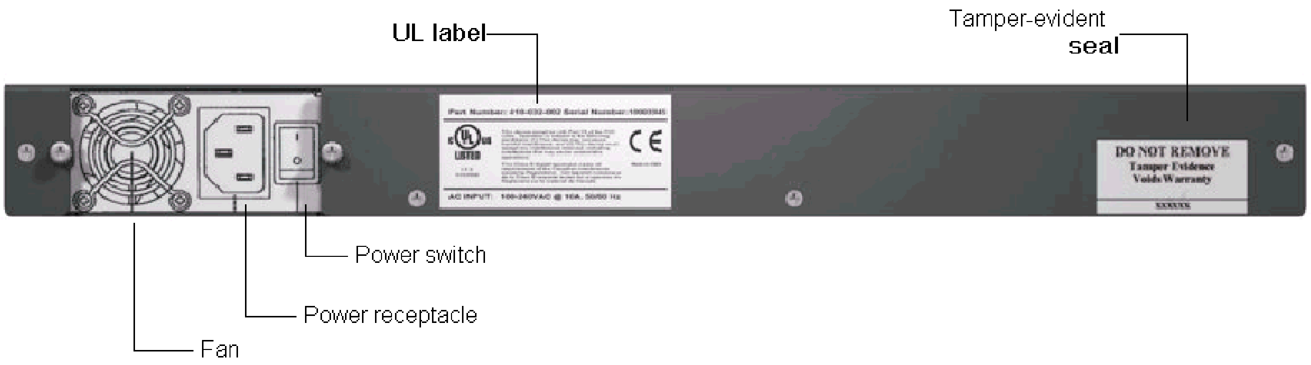

Figure 2. Rear Panel Tamper Seal, HA4000

4.4 Strength of Function

Within the cryptographic security boundary, the HighAssurance 4000 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 HighAssurance 4000 Gateway's network address will be discarded. The HighAssurance 4000 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 Crypto Security Officer and User Guidance

Service	Access Interface		Role Permissions		
	CLI	GUI	CSOA	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 (CSOA)

The Crypto Security Officer A is the individual responsible for controlling access to the HighAssurance 4000 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

Network User (User)

The Network User is a HA4000 device that has authenticated with a remote HA4000 device to perform encryption/decryption services between one or more HA4000s

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 HighAssurance 4000 Gateway are operated in a safe and effective manner. The HighAssurance 4000 Gateway Security Policy shall be applied to all IP data flows through the HighAssurance 4000 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. 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," (Supersedes 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	Updated firmware version to 4.0	CB-xxx	Mm/dd/yy
D	Updated firmware version to 5.1		7/08/08