


# FIPS 140-2 Security Policy

## Extreme Networks Sentriant CE150

**Firmware Version 3.2**  
**Hardware Version A**

<b>ECO, Date, and Revision History</b> Rev A DO-xxx, 05/09/06, Isr Initial release	Contact: Lynn Remaklus		 3585 Monroe St. Santa Clara, CA 95051	
	Checked:	Approved:		
	Filename: 007-003-301a[rev2].doc			
	Title: <b>FIPS 140-2 Security Policy Extreme Networks Sentriant CE150</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:	Document Number:	Rev:	Sheet:
	<b>12-13-2006</b>	<b>007-003-301</b>	<b>A</b>	<b>1 of 15</b>

**Table of Contents**

1 Introduction to the Sentriant CE150 Security Policy ..... 3

2 Definition of the Sentriant CE150 Security Policy ..... 4

    2.1 Sentriant CE150 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 Constraints ..... 7

        2.4.2 Security Policy Limitation ..... 7

        2.4.3 Discretionary Access Control..... 7

        2.4.4 Default Deny ..... 7

        2.4.5 Power Requirements ..... 7

        2.4.6 Security Modes ..... 7

        2.4.7 Physical Level Security ..... 7

    2.5 Secure Setup Procedure..... 7

    2.6 Initiating FIPS Compliant Mode ..... 8

3 Purpose of the Sentriant CE150 Policy ..... 8

    3.1 Sentriant CE150 Security Feature Overview ..... 8

    3.2 Module Self-Tests ..... 10

4 Specification of the Sentriant CE150 Security Policy..... 10

    4.1 Identification and Authentication Policy ..... 11

    4.2 Access Control, Roles, and Services..... 11

    4.3 Physical Security Policy ..... 12

    4.4 Strength of Function ..... 13

5 Glossary of Terms ..... 13

6 References ..... 14

7 Revisions ..... 14

    7.1 Revision History ..... 15



**Figure 1. Sentiariant CE150**

## 1 Introduction to the Sentiariant CE150 Security Policy

This document describes the security policy of the Extreme Networks® Sentiariant™ CE150 encryption appliance as required and specified in the NIST FIPS-140-2 standard. Under the standard, the Sentiariant CE150 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 3.2.

The Sentiariant CE150 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 Sentiariant CE150 security policy, which includes:

- an overview of the Sentiariant CE150 operation
- a list of security rules (physical or otherwise) imposed by the product developer

A description of the purpose of the Sentiariant CE150 security policy, which includes:

- a list of the security capabilities performed by the Sentiariant CE150

Specification of the Sentiariant CE150'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

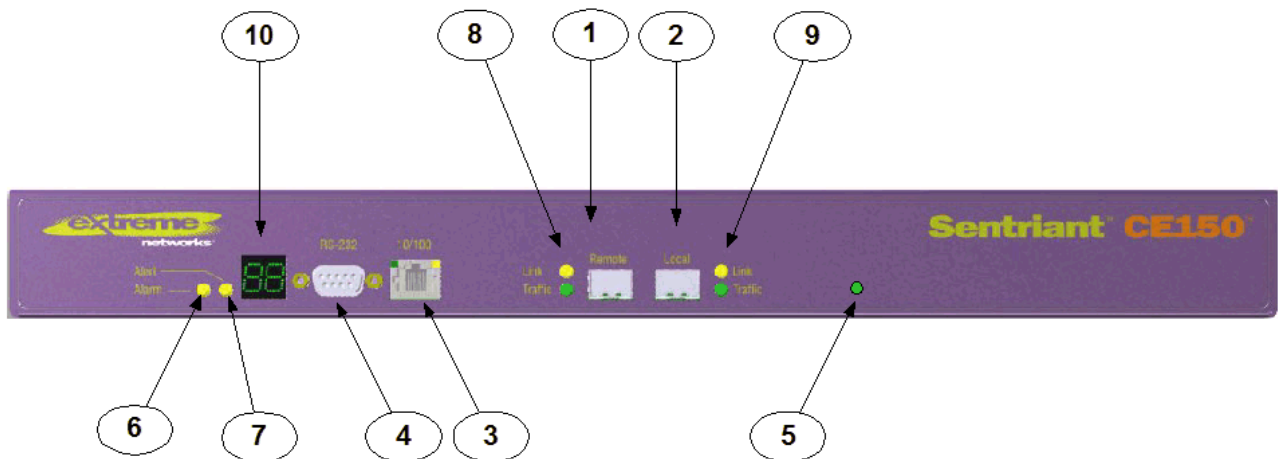
## 2 Definition of the Sentriant CE150 Security Policy

### 2.1 Sentriant CE150 Operation Overview

The Sentriant CE150 is a high performance, integrated security appliance that offers Gigabit Ethernet IPsec encryption. Housed in a tamper evident chassis, the Sentriant CE150 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 Sentriant CE150 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.

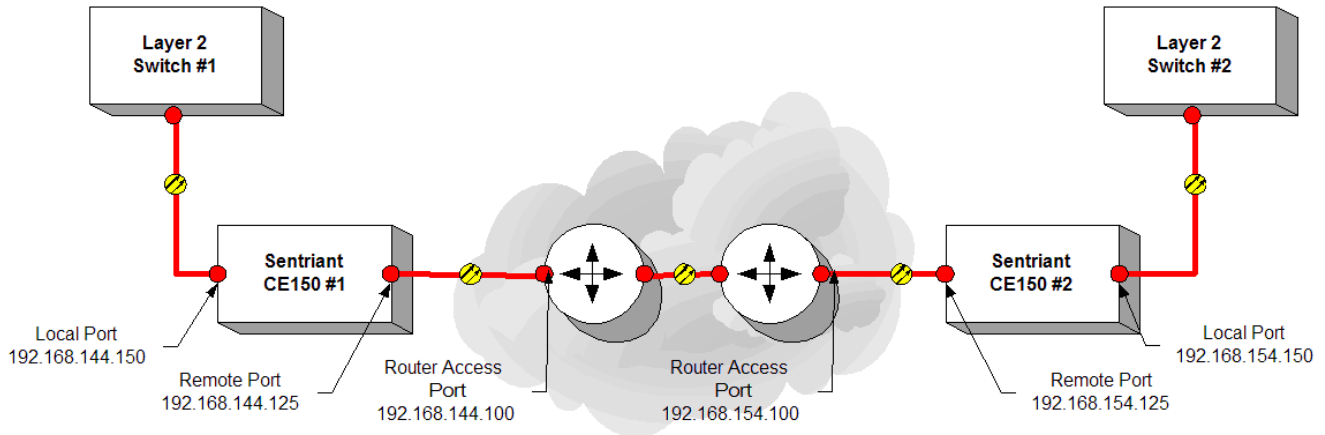
Figure 2 shows the physical layout of the Sentriant CE150. The back of the module (not displayed) contains a standard, enclosed line cord receptacle and cannot be exploited.



**Figure 2. Sentriant CE150 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

A typical operating environment is illustrated in Figure 3.



**Figure 3. Typical operational configuration in which traffic is encrypted between the remote ports of Sentriant CE150 #1 and Sentriant CE150 #2.**

## 2.2 Product Features

### Hardware-based IPsec encryption processing

- Low latency
- 1024 concurrent tunnels

### Line rate Gigabit Ethernet

- Full duplex 1.8 Gbps 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**

<i>Approved or Allowed Security Function</i>	<i>Certificate</i>
<b><i>Symmetric Key Encryption</i></b>	
<b>AES (CBC (e/d; 128, 192, 256))</b>	156
<b>Triple-DES (TCBC (e/d; KO 1,2,3))</b>	258
<b><i>SHS</i></b>	
<b>SHA-1 byte-oriented</b>	117
<b>HMAC-SHA-1</b>	34
<b><i>Asymmetric Keys</i></b>	
<b>RSA (PKCS#1) (Sig Gen and Sig Ver)</b>	79
<b>Random Number Generation (FIPS 186-2)</b>	112
<b>Diffie-Hellman (key agreement, key establishment methodology provides 80 bits of encryption strength)</b>	

<b>Non-Approved Security Function</b>	
<b>MD5</b>	
<b>HMAC MD5</b>	
<b>DES (non-compliant)</b>	

#### 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

## 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 Sentriant CE150 is bound by the following rules of operation to meet FIPS 140-2 Level 2 requirements.

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>12-13-2006</b>	Document Number: <b>007-003-301</b>	Rev: <b>A</b>	Sheet: <b>6 of 15</b>
--	----------------------------	--	------------------	--------------------------

### 2.4.1 Operational Constraints

The Sentries CE150 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.

- Sentries CE150 User Guide
- Sentries CE150 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 Sentries CE150 must always use FIPS approved encryption and message authentication – AES, Triple-DES, and SHA1.

The Sentries CE150 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 Sentries CE150 shall be installed in a controlled area with authorized personnel access only.

## 2.5 Secure Setup Procedure

The Sentries CE150 must be set up, installed, and operated in accordance with the instructions in the User Guide.

- Sentries CE150 User Guide
- Sentries CE150 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 Sentries CE150 User Guide, Version 3.2. 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 Sentries CE150 is shipped with all encryption mechanisms disabled to allow installation test and acceptance. Prior to operation, encryption mechanisms should be enabled.

The Sentries CE150 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](http://www.microsoft.com))

The Sentriant CE150's tamper-evident seal must be intact. If the tamper-evident seal is broken, the Sentriant CE150 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 Sentriant CE150CD).
- 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 Sentriant CE150 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 Sentriant CE150 Policy

The Sentriant CE150 is a high performance security appliance that offers IPSec encryption for Gigabit Ethernet (1 Gbps) traffic. The Sentriant CE150 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 Triple-DES algorithms employed by the Sentriant CE150 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 Sentriant CE150 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
Sentriant CE150 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 Sentriant CE150 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)

#### Continuous Random Number Generator Test:

The Sentriant CE150 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 Sentriant CE150 includes a conditional pairwise consistency test (sign and verify operation) every time RSA keys are generated.

#### Firmware Load Test:

The Sentriant CE150 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 Sentriant CE150 Security Policy

Three roles, which either provide security services or receive services of the Sentriant CE150, are the basis of the specification of the Sentriant CE150 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.

**Crypto Security Officer A:** The Crypto Security Officer "A" role consists of the Admin user. The role controls access to the Sentriant CE150 by maintaining all role-based userid/password configurations.

**Network User:** The User role uses the security services implemented on the Sentriant CE150. The Network User is any Sentriant CE150 appliance that is authenticated with another Sentriant CE150 appliance to perform encryption and decryption services. The Sentriant CE150 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 Sentriant CE150 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:

**Table 3. Identification/Authentication Policy**

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

Note: Any reference of CSO, CSOA, 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 Crypto Security Officer A may set inactivity time outs for login sessions. The login restrictions apply to the CSO and CSOA. 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 Sentriant CE150 module and includes all internal printed circuit cards, integrated circuitry, and so forth contained within its physical dimensions.

Note: Items highlighted in yellow in Table 4 are Services with description of services detailed directly below highlighted area.

**Table 4. Roles and Services**

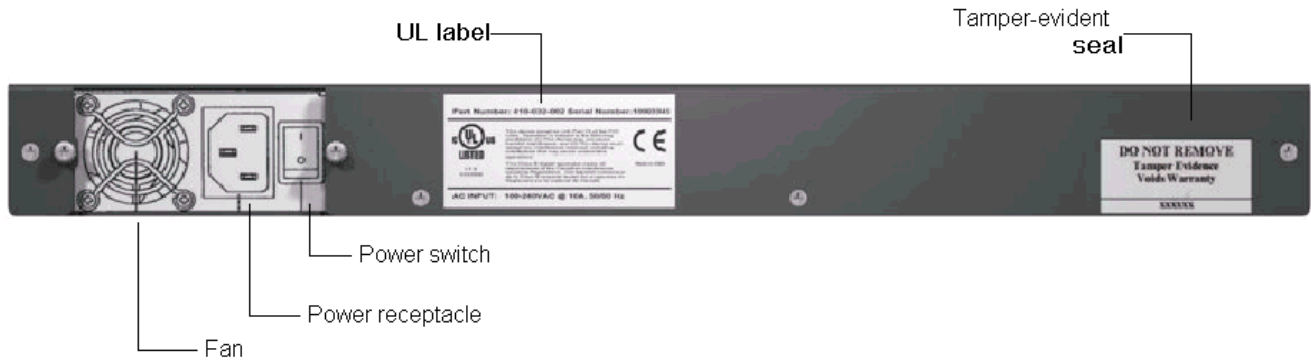
Roles	Service	Security Relevant Data Item	SRDI Access Read, Write, Execute
<b>CSO:</b>	<b>Run Self-Tests</b>		
	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, software authentication, RNG test).	None	Execute
	<b>Key Generation</b>		
	Generate symmetric and asymmetric keys.	Triple-DES, AES, RSA, and Diffie-Hellman	Write, Execute
	<b>Configure</b>		
	Configure IP addresses, subnets, logging, and port settings, set expiration of key lifetime.	None	Read, Write, Execute
	<b>Show Status</b>		
	Display network statistics, network configuration, display port information, display security policy information.	None	Read
	<b>Reboot</b>		

<b>Roles</b>	<b>Service</b>	<b>Security Relevant Data Item</b>	<b>SRDI Access Read, Write, Execute</b>
	Reboot the Sentriant CE150.	None	Execute
	<b>Zeroization</b>		
	Zeroize the Sentriant CE150.	Triple-DES, AES, RSA, Diffie-Hellman, Passwords	Execute
	<b>Update Security Policy</b>		
	Update the security policy rules of the Sentriant CE150.	Triple-DES, AES, RSA	Read, Write
	<b>Load Security Policy</b>		
	Load an updated or saved security policy into the Sentriant CE150.	None	Execute
	<b>Firmware Upgrade</b>		
	Update the firmware of the Sentriant CE150.	RSA	Execute
	<b>Import/Export Key</b>		
	Importing and exporting public keys.	RSA	Execute
<b>CSOA:</b>	<b>Create Passwords</b>		
	Create or change the CSO and CSOA passwords.	Password	Write, Execute
	<b>Set Password Lockout</b>		
	Sets how many attempts a password may be incorrectly entered.	Password	Write
	<b>Run Self-Test</b>		
	Self-test (critical function test, memory test, encrypt hardware test, algorithm self-tests, software authentication, RNG test).	None	Execute
	<b>Load Security Policy</b>		
	Load a saved security policy into the Sentriant CE150.	None	Execute
<b>User</b>	<b>Encrypt/Decrypt</b>		
	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 Sentriant CE150 has been designed 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 4. Sentriant CE150 Rear Panel Tamper Seal**

#### 4.4 Strength of Function

Within the cryptographic security boundary, the Sentriant CE150 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 Sentriant CE150'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 validation.

### 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 Sentriant CE150 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 Sentriant CE150 device that has authenticated with a remote Sentriant CE150 device to perform encryption/decryption services between one or more Sentriant CE150s.

#### 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 Sentriant CE150 are operated in a safe and effective manner. The Extreme Networks Sentriant CE150 Security Policy shall be applied to all IP data flows through the Sentriant CE150, 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.

**6 References**

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

Sentriant CE150 User Guide, Part Number 100225-00, Rev 01, July 2006

Sentriant CE150 Installation Guide, Part Number 100224-00, Rev 01, July 2006

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

**7 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).

### 7.1 Revision History

Revision	Change Description	Change Document	Approved
A	Original Issue	DO-xxx	xx/xx/2006