CIPHEROPTICS

CipherOptics SG-series
Network Security Appliance

Security Target

CipherOptics Inc.; 007-101-001 Revision A
February 8, 2005

REVISION HISTORY

Date of Issue	Revision Number	Description of Change
December 03, 2004	007-101-001 Revision 9	Incorporated DOMUS OR 01 Comments
February 4, 2005	007-101-001 Revision 10	Incorporated CSE OR 01 Comments
February 8, 2005	007-101-001 Revision A	Transferred revision control from AEPOS to CipherOptics, update corporate ID.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ANNEXES

1. INTRODUCTION TO THE SECURITY TARGET

1.1 Security Target Identification

Title:	CipherOptics SG-series Security Target
Product:	CipherOptics SG-series Network Security Appliance Version 3.1 – Models SG100 and SG1002
ST Revision Number:	A
Manufacturer:	CipherOptics

1.2 Security Target Overview

This ST describes the IT security requirements for the CipherOptics™ SG-series Network Security Appliance Version 3.1 – Models SG100 and SG1002 [1]. The CipherOptics SG-series appliances, also referred to as CipherOptics SGx, are encryption appliances that provide end-to-end data security for IP-based network traffic between remote sites across an unsecured wireless or wireline network.

Compliant with the Internet Protocol Security (IPSec) standard (RFC 2401), the CipherOptics SGx provides 3 levels of security:

- Confidentiality – Industry standard algorithms encrypt data: AES, 3DES and DES encryption;
- Integrity – Hash algorithms prevent the undetected alteration of data as it traverses the network: HMAC- SHA-1-96 and HMAC-MD5-96
- Authentication – X.509 v3 digital certificates and the digital signature standard (DSS) are used to verify the identity of the peer IP gateway that is the source of the data.

Key management is provided by Internet Key Exchange (IKE), manual keys, and Diffie-Hellman Groups 1, 2 and 5.

1.3 CC Conformance Claim

The Target of Evaluation (TOE) is conformant with:

1. CC Version 2.2 Part 2-extended. The following non-Part 2 Security Functional Requirement is included to meet a specific requirement of the TOE:
    - FAU_ADG. 1 – Audit data Generation

[1] The platforms vary in assembly, packaging and performance but not in functionality or design. The platforms are therefore, cryptographically equivalent and provide the same security functionality.

- CC Version 2.2 Part 3

1.4 Protection Profile Conformance Claim

This ST does not claim conformance to any Protection Profile.

1.5 Security Target Organization

The main sections of the ST are the target of evaluation (TOE) description, TOE security environment, security objectives, IT security requirements, TOE summary specification, rationale, and annexes.

The TOE description provides general information about the TOE, defines the evaluated configuration for the TOE, and serves as an aid to understanding its security requirements.

The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

- assumptions regarding the TOE's intended usage and environment of use;
- threats relevant to secure TOE operation; and
- organizational security policies with which the TOE must comply.

The security objectives reflect the stated intent of the TOE and its environment. They pertain to how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

The security requirements section provides the IT security requirements as follows:

- TOE security functional requirements (SFRs);
- TOE security assurance requirements (SARs); and
- IT environment security functional requirements.

The TOE summary specification (TSS) provides a description of the TOE security functions (TSF) that the TOE provides in order to satisfy the SFRs. The TSS also describes the assurance measures that will be used to satisfy the SARs. The determination of whether or not the TSFs and SARs satisfy the security requirements is the objective of the TOE evaluation.

The rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The rationale is in three main parts. First, a security objectives rationale

demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a security requirements rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them. Finally, a TOE summary specification rationale demonstrates that the TOE security functions and assurance measures are traceable to the security requirements and are suitable to meet them.

1.6 Related Standards and Documents

1. Common Criteria Version 2.2 - Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements.

2. Common Methodology for Information Security Evaluation (CEM), CEM-99/045, Part 2: Evaluation Methodology, Version 1.0.

3. Security Architecture for the Internet Protocol, RFC 2401, Internet Engineering Task Force (IETF), November 1998.

4. Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, IETF, 1998.

5. The Internet Key Exchange (IKE), RFC 2409, IETF, November 1998.

6. Federal Information Processing Standards Publication (FIPS PUB) 197, November 26, 2001.

7. FIPS PUB 140-2, May 25, 2001.

2. TARGET OF EVALUATION DESCRIPTION

The Target of Evaluation (TOE) is the CipherOptics SG-series Network Security Appliance Version 3.1 – Models SG100 and SG1002. The TOE boundary is considered to be the physical perimeter of the appliance including the outer casing.

2.1 Features

The CipherOptics SGx is an encryption appliance that secures IP-based network traffic while it is in transit across an unsecured wireless or wireline network. Operating at Gigabit Ethernet (CipherOptics SG1002) and Fast Ethernet (CipherOptics SG100) wire-speeds, the CipherOptics SGx protects site-to-site links that transmit information where a delay caused by encryption can affect data quality.

The CipherOptics SGx is housed in a tamper evident chassis, and complies with the IPSec standard (RFC 2401) to provide security services. IPSec is a framework of standards developed by the IETF to support the secure exchange of packets at the IP layer.

2.1.1 IPSec Security Services

The CipherOptics SGx applies security to IP layer traffic as described in RFC-2401, Security Architecture for the Internet Protocol. By utilizing IPSec, the CipherOptics SGx is able to provide the following data security services.

- **Integrity.** Integrity services protect the data in transit from undetected unauthorized modification, ensuring that the data received is exactly the same data that was sent. Hash message authentication codes (HMAC) sign each packet with a cryptographic checksum using a shared, secret key. Only the sender and receiver have the key that is used to calculate the checksum. If the packet contents have changed, the checksum verification fails and the packet is discarded. The CipherOptics SGx uses the Secure Hash Algorithm (SHA-1) for the hash function. The SHA-1 calculation results in a 160-bit hash that is used for the integrity check.

- **Confidentiality.** Confidentiality services ensure that data is not made available or disclosed to unauthorized individuals, entities, or processes. This is achieved by encrypting the data before transmission, ensuring that the data cannot be read during transmission, even if the packet is monitored or intercepted. The CipherOptics SGx uses the Advanced Encryption Standard (AES) encryption algorithm.

- **Data Origin Authentication.** Authentication services provide verification that a message could only have been sent from a computer that has knowledge of the shared, secret key. The receiver can therefore authenticate the identity of the sender. The sender includes (with the message) a message authentication code with a calculation that includes the shared, secret key. The receiver performs the same calculation and, if the receiver's calculation does not match the message authentication code that is included in the message, the message is discarded. This service is dependent upon the data integrity service. X.509 v3 certificates are used for authentication in security policies on the CipherOptics SGx.

- **Anti-replay**. Also known as replay prevention, anti-replay ensures that if an attacker captured data, the data could not be reused or replayed to establish a session illegally. This service prevents attempts to intercept a message and then use the identical message illegally. CipherOptics SGx users can detect and reject replayed packets.

- **Key management**. The Internet Key Exchange (IKE) standard (RFC-2409) is used for centralized security association management and generating and managing shared, secret keys.

- **Tunnel mode**. The CipherOptics SGx operates in tunnel mode. Tunnel mode protects the entire IP packet including the IP header. In tunnel mode the outer IP source and destination addresses identify the endpoints of the tunnel.

- **IPSec Protocol.** The CipherOptics SGx uses Encapsulating Security Payload (ESP) for protecting IP packets. ESP provides data integrity, data origin authentication, limited anti-replay protection and confidentiality (encryption).

2.2 CipherOptics SGx Traffic Flow

Packets that arrive on the Local (trusted) port are generally encrypted then output through the Remote (untrusted) port. Before secured data can be exchanged, a security agreement must be established. The resulting agreement, known as a Security Association (SA), stipulates how to exchange and protect the information being transmitted. Two SAs are established for each connection, one for inbound[2] communication and one for outbound[3] communication.

When sending an outbound packet from the trusted network to the untrusted network, the CipherOptics SGx checks its security policy database (SPD) to determine which SA to use. The SA determines the security processing required for the packet. Management software populates the database according to parameters established by the CipherOptics Policy Management application. If the packet does not match a specified policy, the CipherOptics SGx discards it.

For inbound packets, the CipherOptics SGx examines each packet it receives and takes one of the following actions:

- **Clear Text**. Packets that match a clear text policy are passed unencrypted.

- **Discard**. Packets that match a discard policy are dropped and do not exit the CipherOptics SGx.

- **Encrypt.** For packets that match an encrypt policy the database is consulted to determine whether an SA exists. If an SA does exist the packet is processed according to the encryption parameters specified by the SA. If an SA has not been established the packet goes through the IKE protocol process to establish one. Once the SA is established the packet is processed with the encryption parameters the new SA specifies.[4]

- **Decrypt**. When an encrypted IP packet arrives at the remote port, its security Policy Index (SPI), source IP address and destination IP address are extracted from the

[2] Refers to network packets entering the TOE regardless of origin
[3] Refers to network packets leaving the TOE regardless of destination
[4] This policy is required for secure mode.

encryption IP header. The associated SA is fetched from database using the destination, protocol and SPI. If there is no SA the packet is dropped. If an SA is found the packet is processed with the encryption and authentication attributes specified by the SA.

2.3 Evaluated Appliance Configurations

The following CipherOptics SGx configurations have been evaluated.

Table 2.1 - CipherOptics SGx Evaluated Configurations

Model	Hardware Version	Firmware
CipherOptics SG100	Revision A	3.1
CipherOptics SG1002	Revision A	3.1

2.4 Security Environment

For the purpose of this ST, the CipherOptics SGx is configured and operated in the following deployments:

- Using a layer 2 switch in a back to back configuration
- At layer 3 in a routed network

To secure the data traveling between two sites a CipherOptics SGx is deployed at each site, with complementary security policies configured on each appliance. Traffic is encrypted between the two CipherOptics SGx appliances over an untrusted network, providing end-to-end data security.

Cleartext packets from the trusted network enter the TOE on the Local port. The TOE encrypts the packet and sends it out the Remote port to the untrusted network. At the destination TOE, the encrypted packet enters the Remote port. The destination TOE decrypts the packet and sends it out the Local port to the trusted destination network.

2.5 Secure Mode Configuration

The required configuration in which the CipherOptics SGx is to be evaluated is described as follows.

2.5.1 Management Station[5]

In secure mode, the management station is an IPSec client that interfaces with the TOE. A prerequisite to entering secure mode is to configure the management IP address via a direct connection to the serial port

The IPSec client manages the CipherOptics SGx via the 10/100 Ethernet port. The 10/100 port can be attached to a router or switch or directly to the management station. Regardless of the IPSec client that is used on the management station, it is configured with the same IPSec Policy as the TOE (see Section 2.5.3).

The Network Manager uses the management station to enter and modify security policies, configure the physical interfaces and other operational parameters, and control the operation of the CipherOptics SGx.

- Text-based Command Line Interface (CLI) configures the CipherOptics SGx operating parameters. In secure mode the CLI sessions are managed by a Telnet session secured in an IPSec tunnel to the 10/100 port.
- Browser-based Policy Manager application configures and manages security policies, and manages certificates. Policy Manager sessions are HTTP sessions secured in an IPSec tunnel to the 10/100 port.

2.5.2 Network Traffic

The Network Manager configures security policies for the network traffic on the data path. Based on the filters and security policies that the Network Manager defines, the CipherOptics SGx takes one of the following actions on unicast IP-based packets:

- Discards the packet
- Passes the packet in the clear
- Encrypts the packet

In secure mode, encrypted traffic must be secured using the IPSec policy described in Section 2.5.3.

2.5.3 IPSec Policy

The Network Manager defines the range of traffic to encrypt. To operate in secure mode, encrypted traffic must use the IPSec policy specified below.

[5] Management station is not part of the TOE and does not provide security functionality.

Table 2.2 - CipherOptics SGx IPSec Policy

Parameter	Value
Mode	Tunnel
Authentication	Certificates
IKE Phase 1	
Cipher algorithm	AES-256
Hash algorithm	SHA-1
Negotiation mode	Main mode
IPSec Phase 2	
IPSec protocol	ESP
Cipher algorithm	AES-256
Hash algorithm	SHA-1

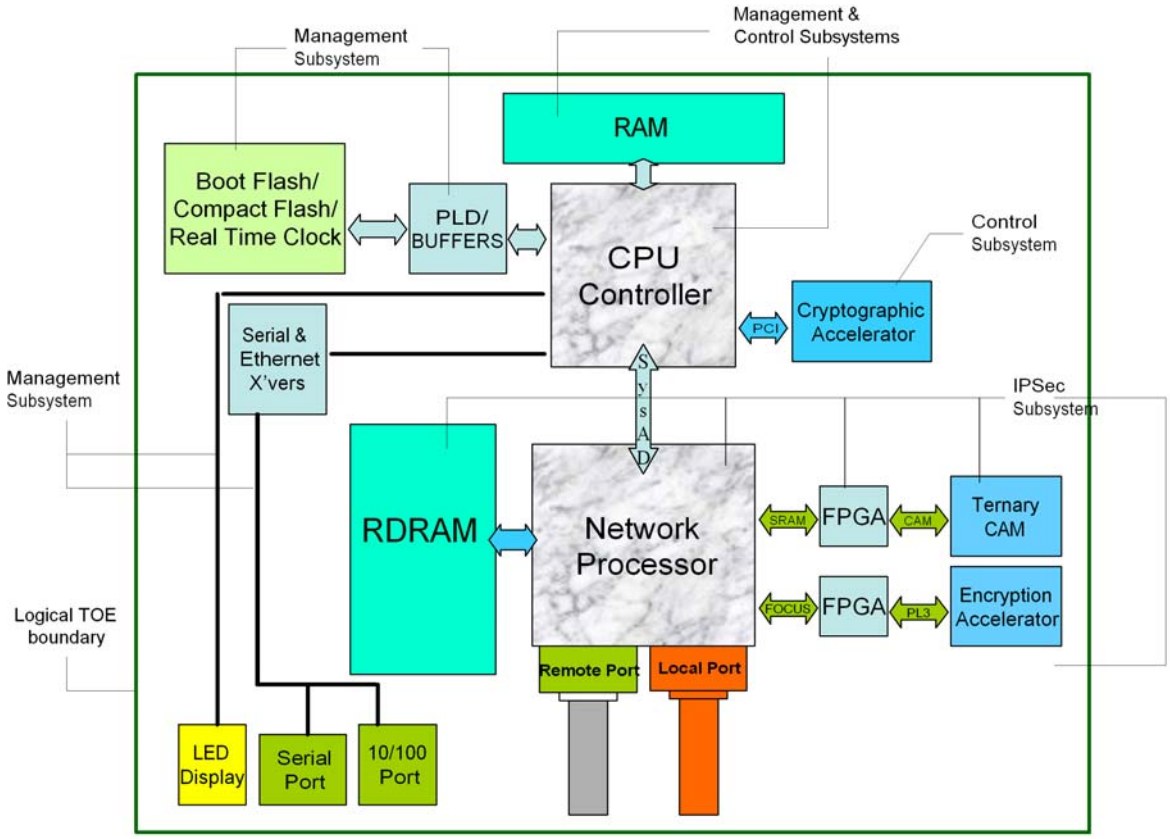
2.5.4 X.509 Certificates

X.509 Version 3 certificates are used for authentication. CipherOptics loads two manufacturing certificates on the appliance, one for use on the data ports and the other for use on the management interface. These certificates are sufficient for secure mode use, or the customer can replace them.

2.6 TOE Functional Description

The TOE is comprised of three subsystems, which are illustrated in the functional block diagram view of the CipherOptics SGx. The sub-systems include: an IPSec Subsystem, a Control Subsystem, and a Management Subsystem. The following paragraphs briefly describe the sub-systems functionality.

Figure 2: TOE Functional Diagram



2.6.1 IPSec Subsystem

The primary function of the IPSec subsystem is to encrypt and decrypt the IP packets being passed through the Remote (untrusted) and Local (trusted) ports of the CipherOptics SGx. If the CipherOptics SGx receives clear text IP packets on the Local port, the packet is passed through the components of the IPSec subsystem, where it is encrypted. The packet is then passed to the physical interface for transmission out of the Remote port. Ciphertext IP packets entering the Remote port side follow a similar reverse path through the IPSec subsystem for decryption.

2.6.2 Control Subsystem

The primary functions of the control subsystem are for key exchange and security association database (SAD) management. The control subsystem implements the control plane for the IPSec protocol, which includes the IKE protocol. The Cryptographic Accelerator includes a device for the random number generator function to assist in generating keys for encrypting and decrypting IP packets.

2.6.3 Management Subsystem

The primary function of the management subsystem is to configure security policies. Secondary functions are to provide an internal interface to the other subsystems and provide a user interface to assign IP addresses to the CipherOptics SGx external interfaces. The management subsystem supports several simultaneous processes. After loading the OS the system automatically initiates a CipherOptics SGx daemon process that controls the operation of the system's Local and Remote network interfaces and its associated cryptographic functions. The processor is also responsible for establishing the Network Manager session via the serial port or the 10/100 Ethernet management port. Commands entered by the Network Manager as part of a session are interpreted by the CPU and passed to the CipherOptics SGx daemon for execution.

3. TOE SECURITY ENVIRONMENT

This section identifies the security problem that exists with the protection of identified assets. The security problem is expressed as threats and policy that the TOE, operating in its environment, must address. For the TOE to fulfill its security requirements, specific conditions must be upheld in the operating environment. These conditions are expressed as assumptions.

3.1 Assets

The assets of concern to this ST are defined as follows:

- **Users**. Users are defined as any entity with an assigned IP address that matches the module's IPSec policy as defined by the Network Manager.

- **Administrative Users.** Administrative users are defined as those users required to configure and manage the TOE. For the purpose of the ST these users are identified as the Network Manager and the Administrator.

- **Information.** IP data packets represent the information to be protected.

- **TSF data.** TSF data is defined as data that is required to support the secure operations on the IP packets. It includes the security parameters required for operation of the IPSec function. These parameters include the following: encryption algorithm, integrity algorithm, authentication method, IPSec protocol, Administrator and Network Manager passwords.

Assets are to be protected in terms of confidentiality and integrity. Additional security services such as anti-replay and data origin authentication are also to be provided for assets.

3.2 Statement of Assumptions

The specific conditions listed below are assumed to exist in the CipherOptics SGx operating environment. Each assumption is stated in bold type font. An application note, in normal font, which supplies additional information and interpretation, follows it.

3.2.1 Personnel Assumptions

A.TRUSTED_ADMIN

The system administrative personnel are trusted and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator/user documentation. Furthermore, the administrators of the TOE have been adequately trained in order for them to securely configure the TOE.

3.2.2 Physical Assumptions

A.PHYSICAL

The TOE resides in a physically secure environment.

3.3 Statement of Threats

The following threats are addressed by the TOE operating in its intended environment or by technical security measures provided by the environment or by non-technical security measures (personnel, procedural and physical measures) in the environment.

T.REPLAY

An unauthorized person may capture data and attempt to reuse or replay the data to establish an illegal session with the TOE.

T.DISCLOSE

An unauthorized person may intercept and read data within a packet flow transmitted and/or received by the TOE when traveling over an untrusted network.

T.MODIFY

An unauthorized person may intercept and modify packet flows transmitted/received by the TOE when traveling over an untrusted network.

T.SPOOF

An unauthorized person may attempt to impersonate the identity (IP address) of a trusted system.

T.ACCESS_TOE

An unauthorized person may gain access[6] to the TOE and compromise its security functions by changing its configuration.

3.4 Organizational Security Policy

Each policy is stated in bold type font, and is followed by an application note, in normal font, which supplies additional information and interpretation.

P.TAMPER_SEAL

The Network Manager is required to check the tamper seal (which is applied by CipherOptics) periodically in order to detect any physical attempts to compromise the security functions of the TOE.

P.CONNECT

The TOE security policy configured by the Network Manager will determine whether networks connected to the TOE are trusted or untrusted, identify which packet flows are to be protected by the TOE, and relate each protected packet flow with a peer TOE that will decrypt/encrypt the flow.

[6] Access refers to logical access opposed to physical access

4. SECURITY OBJECTIVES

4.1 TOE Security Objectives

This section defines the security objectives of the TOE. Security objectives are categorized as either IT security objectives or non-IT security objectives and serve to reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. Each objective is stated in bold type font. If required, an application note, in normal font, which supplies additional information and interpretation, follows it.

4.1.1 TOE IT Security Objectives

O.ANTI_REPLAY

The TOE must provide mechanisms to detect that an IP packet flow transmitted to the TOE has not been reused or replayed to establish a TOE session illegally.

O.INTEGRITY

The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet flow transmitted to/from the TOE will be detected.

O.CONFIDENTIALITY

The TOE must provide mechanisms to ensure that IP packets transmitted to/from the TOE over an untrusted network are not made available or disclosed to unauthorized individuals.

O. DATA_ORIGIN

The TOE must provide the means for ensuring that an IP packet has been received from a trusted entity.

O.SECURE_PATH

The TOE must provide the means for the trusted and trained Network Manager to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The TOE will apply the parameters included in this policy to provide an IPSec channel compliant with RFC 2401, 2408, 2409 for secure communication.

O.ADMIN

The TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality in a secure manner.

O.TOE_INTEGRITY

The TOE must provide the means for determining the loss of TOE integrity, which could compromise critical security parameters.

4.2 Environmental Security Objectives

4.2.1 IT Environmental Security Objectives

There are no IT security objectives for the environment.

4.2.2 Non-IT Security Objectives for the Environment

The non-IT Environmental security objective is as follows.

OE.PHYSICAL

Those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attack.

OE.TRUSTED_ADMIN

Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.

5. IT SECURITY REQUIREMENTS

This section specifies the Security Functional Requirements (SFRs) for the TOE. All SFRs were drawn from Part 2 of the CC with the exception of FAU_ADG. 1, which is defined as an extended security requirement based on the CC SFR - FAU_GEN.1.

5.1 Audit

5.1.1 Audit Data Generation (FAU_ADG.1)[7]

FAU_ADG.1.1 The TSF shall be able to generate an audit record of the following auditable event:

a) Snmp-trap (successful and unsuccessful login attempts, log outs);
b) [assignment: no other specifically defined auditable events].

FAU_ADG.1.2 The TSF shall record within each audit record at the following information:

a) date and time of the event, type of event and the outcome (success or failure) of the event; and
b) for each audit event type, based on the auditable event definitions of the functional components included in the ST, [assignment: no other audit relevant information].

Rationale: FAU_ADG.1.1 and FAU_ ADG.1.2 are necessary to specify audit requirements as performed by the TOE. FAU_SAR.1 has a dependency FAU_GEN.1. FAU_ADG.1.1 which is an extended security requirement based on FAU_GEN.1, generates the audit record and FAU_ADG.1.2 indicates the information contained within the audit record. The dependency is satisfied because a record has to first be generated before it can be read. The TOE audit function does not record start up and shut down of the audit function so the extended requirement is fulfilling the dependency requirement instead of FAU_GEN.1.

5.1.2 Security Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [Network Manager] with the capability to read [all audit information] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.1.3 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

[7] Extended Security Requirement

5.2 Communication

5.2.1 Enforced Proof of Origin (FCO_NRO.2)

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted [assignment: IP data packets] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [assignment: IP address of the source IPSec peer] of the originator of the information, and the [assignment: X.509 Version 3 certificate] of the information to which the evidence applies.

FCO_NRO. 2.3 The TSF shall provide a capability to verify the evidence of origin of information to [selection: recipient], [assignment: lPSec destination peer] given [assignment: the successful establishment of a SA between the source and destination peers].

5.3 Cryptographic Support

5.3.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: AES algorithm] and specified cryptographic key sizes [assignment: 256] that meet the following: [Federal Information Processing Standards Publication (FIPS PUB) 186-2].

5.3.2 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: erase and overwrite in memory] that meets the following: [assignment: Federal Information Processing Standards Publication (FIPS PUB 140-2].

5.3.3 Cryptographic Operation (FCS_COP.1)

FCS_COP.1.1 The TSF shall perform [assignment: encryption/decryption, message signing, key generation] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm] and cryptographic key sizes [assignment: key sizes] that meet the following: [assignment: list of standards].

Table 5.1 - Cryptographic Operations

Algorithm	Size	Mode	Operation	Standard
AES	256	CBC	Encryption/Decryption	FIPS PUB 197 Advanced Encryption Standard
SHA-1 hash	20 Byte HMAC SHA-1-96	Byte oriented	Message signing	FIPS PUB 180-1 (RFC 2404)
Diffie-Hellman			Key Establishment	RFC 2409

5.4 User Data Protection

5.4.1 Subset Information Flow Control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [assignment: information flow control SFP] on [assignment subject: Secure Communication Session, information: IP data packets, operation: IP packet transmission between TOEs].

5.4.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the [assignment: information flow control SFP] based on the following types of subject and information security attributes: [assignment: the minimum number and type of security attributes].

Subject: Secure Communication Session

Security Attributes: x.509 Version 3 certificates, IP address, IPSec Phase 1 and 2 parameters.

FDP_IFF.1.2 The TSF shall permit an information flow between controlled subjects of controlled information via a controlled operation if the following rules hold: [assignment: a SA is negotiated and agreed upon for the transmission of IP packets between two IPSec peers].

FDP_IFF.1.3 The TSF shall enforce [assignment: no additional information flow control SFP capabilities].

FDP_IFF.1.4 The TSF shall provide the following [assignment: no additional SFP capabilities].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules:
[assignment: rules based on security attributes, that explicitly authorize information flows].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: The TOE will reject any unauthenticated packet flow].

5.4.3 Basic Data Exchange Confidentiality (FDP_UCT.1)

FDP_UCT.1.1 The TSF shall enforce the [assignment: information flow control SFPs] to be able to [selection: transmit and receive] objects in a manner protected from unauthorized disclosure.

5.4.4 Data Exchange Integrity (FDP_UIT.1)

FDP_UIT.1.1 The TSF shall enforce the [assignment: information flow control SFP] to be able to [selection: transmit and receive] user data in a manner protected from [selection: modification, insertion and replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [selection: modification, insertion and replay] has occurred.

5.5 Identification and Authentication

5.5.1 User[8] Authentication Before Any Action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF mediated actions on behalf of that user.

5.5.2 User[9] Identification Before Any Action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

[8] Refers to administrative user.
[9] Refers to administrative user.

5.6 Security Management

5.6.1 Management of Security Attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [assignment: access control SFP] to restrict the ability to [selection: query, modify and delete] the security attributes [assignment: configuration of x.509 Version 3 certificates, IP address, IPSec Phase 1 and 2 parameters] to [assignment: the Network Manager].

5.6.2 Static Attribute Initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [assignment: information flow control SFP] to provide [selection: restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: Manufacturer] to specify alternative initial values to override the default values when an object or information is created.

5.6.3 Management of TSF Data (FMT_MTD.1) - passwords

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: modify] the [assignment: passwords] to [assignment: the Administrator].

5.6.4 Management of TSF Data (FMT_MTD.1) – unsuccessful login attempts

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: query, modify and clear] the [assignment: unsuccessful login attempts] to [assignment: the Administrator].

5.6.5 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: the password management function, unsuccessful login attempts management function, security policy management function].

5.6.6 Restrictions on Security Roles (FMT_SMR.2)

FMT_SMR. 2.1 The TSF shall maintain the roles: [Administrator and Network Manager].

FMT _SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR. 2.3 The TSF shall ensure that the conditions [that each user has to be authenticated as before they can be allowed to assume their role] are satisfied.

5.7 Protection of the TOE Security Functions

5.7.1 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1 The TSF shall be able to provide reliable time stamps for its own use.

5.7.2 Abstract Machine Testing (FPT_AMT.1)

FPT_AMT.1.1 The TSF shall run a suite of tests [selection: during initial start-up] to demonstrate the correct operation of the security assumptions provide by the abstract machines that underlies the TSF.

5.7.3 Passive Detection of Physical Attack (FPT_PHP.1)

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

5.7.4 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.7.5 TSF Domain Separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.8 TOE Access

5.8.1 TOE Session Establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: the following security attributes: x.509 Version 3 certificates, IP address, IPSec Phase 1 and 2 parameters].

5.9 Trusted Path/Channels

5.9.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: the remote trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: management sessions and communication sessions].

5.10 SFR Dependencies

Some of the IT Security Functions described above have dependencies. The following table illustrates that the security target has satisfied SFRs which have dependencies and provides remarks for those which are omitted.

Table 5.2: SFR Dependency Table

Security Functional Requirement	Dependencies	Remarks
FAU_ADG.1[10]	FPT_STM.1	Included
FAU_SAR.1	FAU_ADG.1	Included

[10] Extended requirement based on the CC part 2 functional requirement FAU_GEN.1 which has a dependency on FPT_STM.1. We therefore included this dependency as well.

Security Functional Requirement	Dependencies	Remarks
FAU_SAR.2	FAU_SAR.1	Included
FCO_NRO.2	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1
FCS_CKM.1	FCS_COP.1, FCS_CKM.4, FMT_MSA.2	FCS_COP.1 , FCS_CKM.4 are included. FMT_MSA.2 is not required as there are no modifiable security attributes applicable to this SFR.
FCS_CKM.4	FCS_CKM.1, FMT_MSA.2	FCS_CKM.1 is included. FMT_MSA.2 is not required as there are no modifiable security attributes applicable to this SFR.
FCS_COP.1	FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	FCS_CKM.1, FCS_CKM.4 are included. FMT_MSA.2 is not required as there are no modifiable security attributes applicable to this SFR.
FDP_IFC.1	FDP_IFF.1	Included
FDP_IFF.1	FDP_IFC.1, FMT_MSA.3	Included
FDP_UCT.1	FDP_IFC.1, FTP_ITC.1	Included

Security Functional Requirement	Dependencies	Remarks
FDP_UIT.1	FDP_IFC.1, FTP_ITC.1	Included
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FIA_UID.2	N/A	
FMT_MSA.1	FDP_IFC.1, FMT_SMR.1, FMT_SMF.1	Included
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Included
FMT_MTD.1[11]	FMT_SMR.1, FMT_SFM.1	Satisfied by FMT_SMR.2 which is hierarchical to FMT_SMR.1. FMT_SFM.1 is included.
FMT_MTD.1[12]	FMT_SMR.1, FMT_SFM.1	Satisfied by FMT_SMR.2 which is hierarchical to FMT_SMR.1. FMT_SFM.1 is included.
FMT_SMF.1	N/A	N/A
FMT_SMR. 2	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FPT_STM.1	N/A	N/A

[11] passwords
[12] unsuccessful login attempts

Security Functional Requirement	Dependencies	Remarks
FPT_AMT.1	N/A	N/A
FPT_PHP.1	FMT_MOF.1	This dependency is argued away as passive detection of physical attack is performed by visual inspection opposed to automated inspection.
FPT_RVM.1	N/A	N/A
FPT_SEP.1	N/A	N/A
FTA_TSE.1	N/A	N/A
FPT_ITC.1	N/A	N/A

5.11 TOE Security Assurance Requirements

The assurance requirements for the TOE are as specified in the EAL 2 package. This level was chosen considering the intended operational security environment for the TOE and the existing assurance measures in the development environment. The assurance requirements are summarized in Table 5-3. As none of the IT security assurance requirements are refined, they are not transcribed in the ST. The reader is referred to Part 3 of the Common Criteria.

Table 5.3: Security Assurance Components

Component	Component Name	Refined?
ACM_CAP.2	Configuration items	No
ADO_DEL.1	Delivery procedures	No
ADO_IGS.1	Installation, generation, and start-up procedures	No
ADV_FSP.1	Informal functional specification	No
ADV_HLD.1	Security enforcing high-level design	No
ADV_RCR.1	Informal correspondence demonstration	No
AGD_ADM.1	Administrator guidance	No

Component	Component Name	Refined?
AGD_USR.1	User guidance	No
ATE_COV.1	Analysis of coverage	No
ATE_FUN.1	Functional testing	No
ATE_IND.2	Independent testing - sample	No
AVA_SOF.1	Strength of TOE security function evaluation	No
AVA_VLA.1	Developer vulnerability analysis	No

5.12 Strength of Function Requirement

The claimed strength of function (SOF) against the user[13] authentication password (as described in section 6.1 - ITSF_ADMIN) is SOF-basic. As the TOE is assumed to operate in a secure environment, SOF-basic is consistent with the security objective of the TOE.

The password used at Administrator and Network Manager login is the only probabilistic or permutational function on which the strength of the authentication mechanism depends. The Administrator of the TOE chooses the passwords. The password can range from eight to forty characters in length. Documentation advices that strong passwords are chosen (i.e., mix of upper and lower case, digits ands special characters) Assuming that the user chooses a password comprising eight characters[14], the number of password permutations is:

52 alpha characters (upper and lower)
10 digits
+ 10 special characters (at least)
72 possible values
72^8 = (72*72*72*72*72*72*72*72) = **722,204,136,308,736**

The authentication mechanism is designed with a locking feature. After the third failed authentication attempt the Network Manager is locked out until the Administrator re-sets the password. If the Administrator is locked out the appliance must be returned to the factory.

5.13 Security Requirements for the IT Environment

There are no IT security requirements allocated to the IT environment.

[13] Refers to administrative user
[14] The worst case scenario

6. TOE SUMMARY SPECIFICATION

6.1 Statement of TOE Security Functions

This section contains a listing of the TOE security functions that satisfy the SFRs.

ITSF_ANTI REPLAY

- The TOE applies security to IP layer traffic as described in RFC-2401, 2408 and 2409 for secure communication. IPSec allows the exchange and verification of identities without exposing that information to interpretation by an attacker. Mutual verification (authentication) is used to establish trust between the communicating systems and only trusted systems can communicate with each other. After identities are established, IPSec uses cryptography-based keys, shared only by the sending and receiving computers, to create a cryptographic checksum (SHA-1 HMAC) for each IP packet. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys could have sent each packet. Additionally, all authenticated communication includes a sequence number which will detect replay.

- IPSec defines two security protocols for protecting IP packets (Encapsulating Security Payload (ESP) and Authentication Header (AH)). AH provides data integrity, data origin authentication and anti-replay protection. ESP provides all of the services AH does (integrity, data origin authentication and anti-replay) but also includes encryption. The TOE implements ESP as the IPSec security protocol.

ITSF_INTEGRITY

- IPSec defines two security protocols for protecting IP packets (Encapsulating Security Payload (ESP) and Authentication Header (AH)). The TOE implements ESP as the IPSec security protocol which provides confidentiality, integrity, data origin authentication and anti-replay services. The TOE provides integrity services by implementing SHA-1.

ITSF_CONFIDENTIALITY

- IPSec defines two security protocols for protecting IP packets (Encapsulating Security Payload (ESP) and Authentication Header (AH)). The TOE implements ESP as the IPSec security protocol which provides confidentiality, integrity, data origin authentication and anti-replay services. The TOE provides confidentiality services by implementing the AES cipher.

- The TOE generates cryptographic keys to provide confidentiality services in accordance with the AES algorithm. TOE session keys are destroyed after the SA lifetime has expired. No further communication can take place using an expired key.

ITSF_DATA ORIGIN

- IPSec defines two security protocols for protecting IP packets (Encapsulating Security Payload (ESP) and Authentication Header (AH)). The TOE implements ESP as the IPSec security protocol which provides confidentiality, integrity, data origin authentication and anti-replay services.

- The TOE provides data origin authentication for the communicating TOE's by utilizing x.509 Version 3 certificates.

- The TOE implements data origin services for the IP packet by implementing the SHA-1 hash algorithm to create a cryptographic checksum. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys could have sent each packet.

ITSF_SECURE PATH

- The TOE implements IPSec which uses IP packet filtering methodology as the basis for determining whether communication is allowed, secured, or blocked. The Network Manager defines the range of traffic to encrypt, which is incorporated in the security policy.

- The TOE implements an information flow control policy between two communicating IPSec peers via the IKE protocol. The identity of the peer IP gateway is assured through the IKE standard which establishes a method for creating security associations and key exchange decisions. Phase 1 of IKE establishes a secure authenticated channel between the communicating CipherOptics SGx appliances with assured identification of end-points.

- The TOE implements the IPSec protocol that supports two modes of operation (transport and tunnel mode). The CipherOptics SGx supports tunnel mode, which protects the entire IP packet including the IP header. When IPSec tunnel mode is used, IPSec encrypts the IP header and the payload. Tunnel mode provides the protection of the entire IP packet by treating it as an ESP payload. The entire IP packet is encapsulated with an ESP header and an additional IP header. The IP addresses of the encapsulated IP header are the ultimate source and destination addresses. The encapsulated portion of the packet indicates where the packet has been signed for integrity and authentication. The encrypted portion of the packet indicates what information is protected with confidentiality.

- Traffic from one gateway destined to another will only be forwarded if the connection requests and traffic satisfy the information flow policies (SA) configured in the CipherOptics SGx by the Network Manager. If data received by a CipherOptics SGx does not conform to the policy (SA) it will be discarded immediately.

ITSF_ADMIN

The TOE provides functionality that enables an authorized user[15] to effectively manage the TOE and its security functions.

- In secure mode, the management station is an IPSec client that interfaces with the TOE. A prerequisite to entering secure mode is to configure the TOE's management IP address via a direct connection to the serial port. The IPSec client manages the CipherOptics SGx via the 10/100 Ethernet management port. The 10/100 Ethernet management port can be attached to a router or switch or directly to the management station. Regardless of the IPSec client that is used on the management station, it is configured with the same IPSec Policy as the TOE (see Section 2.5.3). The Network Manager uses the management station to enter and modify security policies, configure the physical interfaces and other operational parameters, and control the operation of the CipherOptics SGx.

  - Text-based Command Line Interface (CLI) configures the CipherOptics SGx operating parameters. In secure mode the CLI sessions are managed by a Telnet session secured in an IPSec tunnel to the 10/100 Ethernet management port.

  - Browser-based Policy Manager application configures and manages security policies, and manages certificates. Policy Manager sessions are HTTP sessions secured in an IPSec tunnel to the 10/100 Ethernet management port.

- The TOE provides reliable timestamps via the appliance's internal real time clock and system clock.

- The audit function records log file contents in a file and/or on the terminal. Viewing of the log files is restricted to the Network Manager. The following Audit event is recorded:

  - snmp-trap - successful and unsuccessful login attempts, log outs.

- The TOE provides two roles for managing its security functions: the Administrator and the Network Manager. The Administrator is responsible for password management functions and limiting unsuccessful login attempts. The Network Manager is responsible for configuring the TOE and its security policies to secure the data and management paths.

[15] The user type referenced here refers to the CipherOptics Administrator and Network Manager.

- Default passwords must be changed from their initial values. The administrator logs in first and sets the Administrator and Network Manager's password. The passwords must be at minimum eight characters in length but can be up to forty characters in length. Three-failed log in attempts are permitted.

- The TOE requires the Administrator and Network Manager to enter a correct username and password before allowing any action to take place.

- The restrictive default values as defined for the secure mode configuration ensure that only secure values are accepted for security attributes. The security attributes referenced here refer to key algorithms, modes and lengths. The Network Manager is the only operator with the capability to override the default values.

ITSF_TOE INTEGRITY

The TOE provides the means for determining the loss of TOE integrity, which could compromise critical security parameters via the following functionality.

- The TOE runs a suite of FIPS 140-2 defined self-tests during initial start-up to demonstrate the correct operation of the security functions provided by the abstract machine. The self-tests include the following:
-

The Management subsystem –

- CRC-32 performed on bootrom data
- RAM test
- File system missing
- Application image authentication

The Control Subsystem -

- CRC-32 performed on bootrom data
- RAM test
- Random Number test
- Cryptographic Accelerator self test
- Application image authentication

The IPSec Subsystem -

- CRC-32 performed on bootrom data
- NPU initialization/quick test
- RDRAM initialization test
- RDRAM test
- CAM test
- Encryption Accelerator 3DES/SHA-1 algorithm test

  - Encryption Accelerator AES/SHA-1 algorithm test
  - Application image authentication

- The TOE will preserve a secure state when a self-test or power failure occurs. If any of the tests listed above fail, the boot process is halted. Therefore, no IPSec Policies are loaded, and the network data interfaces are not enabled. This ensures that the CipherOptics SGx cannot perform any cryptographic operations or output any data. If a login failure occurs the operator is locked out until the Administrator re-sets the password.

- The CipherOptics SGx has two ports for processing data traffic; they are called the Remote port and the Local port. The CipherOptics SGx is cabled to the network such that the Remote port is connected to the untrusted network, and the Local port is connected to the trusted network. All packets traversing from the untrusted network to the trusted network enter the CipherOptics SGx via the Remote port and exit via the Local port. Similarly, packets traversing from the trusted network to the untrusted network enter the CipherOptics SGx via the Local port and exit via the Remote port. The CipherOptics SGx inspects all packets traversing the trusted network to the untrusted network, and packets traversing the untrusted network to the trusted network. There is no mechanism to bypass packet inspection. The process of packet inspection involves observing the packet's source and destination IP address, the TCP source and destination port, and the protocol field of the IP header. With this information, a predefined policy is searched for which was configured by the Network Manager.

- The TOE provides a tamper seal. The Network Manager by policy definition is required to check the tamper seal periodically in order to detect any physical attempts to compromise the security functions of the TOE.

6.2 Statement of Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements.

- Configuration Management Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

Table 6.1: Security Assurance Components

Assurance Requirements	Rationale
AM_ACM_CAP	A configuration management system for the development process is used and this is documented indicating that the TOE was developed using this CM system.
AM_ADO_DEL	Secure delivery procedures are documented.
AM_ADO_IGS	Installation procedures to securely install the TOE are provided. A secure mode of operation is described to ensure the TOE is operating in secure mode.
AM_ADV_FSP	A functional specification document is provided that describes each security function in the ST. External interfaces are described along with functional behaviour at these interfaces. Error and exception handling is also described.
AM_ADV_HLD	A document is provided that describes the TOE functionality in subsystems. Interfaces are also described.
AM_ADV_RCR	A document is provided that maps the functions in the high level design to the functional specification and from the functional specification to the TOE summary specification.
AM_AGD_ADM	A user manual is provided that indicates the administrator's role and services.
AM_AGD_USR	A user manual is provided that indicates the user's role and services.
AM_ATE_COV	A coverage document is provided that maps the tests done during development to the functional requirements in the ST.
AM_ATE_FUN	A test plan and test cases that test each of the security functions in the ST are provided.
AM_ATE_IND	This is provided by the evaluation laboratory.
AM_AVA_SOF	A document describing the strength of function of passwords used is provided.
AM_AVA_VLA	A vulnerability assessment is provided that examines the TOE in its environment and indicates how the vulnerabilities are mitigated.

7. RATIONALE

This section demonstrates that TOE security functions and assurance measures are effective at solving the security problem defined for the environment in terms of threats, policies and assumptions. The approach is one of pair-wise refinement, whereby the stated security objectives are shown to be effective against the security problem, the security requirements are shown to satisfy the security objectives, and finally that the TOE summary specification is sufficient to meet the security requirements.

7.1 Security Objectives Rationale

This section demonstrates that the stated security objectives address all identified assumptions, threats, or policies. Table 7-1 demonstrates that each security objective covers at least one assumption, threat or policy, and that each assumption, threat and policy is covered by at least one security objective.

Table 7.1: Summary of Correspondence Between Threats/Assumptions/Policies and SO's

Assumptions/Threats/Policies	O.ANTI_REPLAY	O.INTEGRITY	O.CONFIDENTIALITY	O.DATA_ORIGIN	O.SECURE_PATH	O.ADMIN	O.TOE_INTEGRITY	OE.TRUSTED_ADMIN	OE.PHYSICAL
A.TRUSTED_ADMIN								X	
A.PHYSICAL									X
T.REPLAY	X				X				
T.DISCLOSE			X		X				
T.MODIFY		X			X				
T.SPOOF				X	X				
T.ACCESS_TOE							X		
P.TAMPER_SEAL							X		
P.CONNECT					X	X			

7.1.1 Security Objectives Sufficiency

This section demonstrates the sufficiency of the Security Objectives.

7.1.1.1 Assumptions

A.TRUSTED_ADMIN assumes that system administrative personnel are trusted, not careless, willfully negligent, or hostile and will follow and abide by the instructions provided in the administrator documentation. Furthermore, it assumes that the administrators of the TOE have been adequately trained in order for them to securely configure the TOE. This assumption is addressed by the **OE.TRUSTED_ADMIN** objective which states that those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.

A.PHYSICAL assumes the TOE operating environment is physically secure. This assumption is addressed by the **OE.PHYSICAL** objective which states that those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attack.

7.1.1.2 Threats

T.REPLAY states that an unauthorized person may capture data and attempt to reuse or replay the data to establish an illegal session with the TOE. This threat is countered by **O.ANTI_REPLAY** which ensures that the TOE provides mechanisms to detect that an IP packet flow transmitted to the TOE has not been reused or replayed to establish a TOE session illegally. **T.REPLAY** is countered by **O.SECURE_PATH** which states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE will be able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication.

T.DISCLOSE states that an attacker may attempt to disclose data within a packet flow transmitted and/or received by the TOE when traveling over an untrusted network. This threat is countered by the **O.CONFIDENTIALITY** objective which ensures that the TOE will provide mechanisms to ensure that IP packets transmitted to/from the TOE over an untrusted network are not made available or disclosed to unauthorized individuals. It is also countered by **O.SECURE_PATH** which states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE will be able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication.

T.MODIFY states that an attacker may attempt to modify packet flows transmitted/received by the TOE when traveling over an untrusted network. This threat is countered by the **O.INTEGRITY** objective which ensures that TOE will provide mechanisms to ensure that any attempt to corrupt or modify an IP packet flow transmitted to/from the TOE will be detected. It is also countered by **O.SECURE_PATH** which states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE will be able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication.

T.SPOOF states that an attacker may attempt to impersonate the identity (IP address) of a trusted system. This threat is countered by the **O.DATA_ORIGIN** objective which ensures that the TOE will provide the means for ensuring that an IP packet has been received from a trusted entity. It is also countered by **O.SECURE_PATH** which states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE will be able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication.

T.ACCESS_TOE states that an attacker could gain logical access to the TOE and compromise the TOE security functions by altering its configuration. This threat is countered by the **O.TOE_INTEGRITY** objective which states that the TOE must provide the means for determining the loss of TOE integrity which could compromise critical security parameters.

7.1.1.3 Policies

P.TAMPER_SEAL requires that the Network Manager is required to check the tamper seal in order to detect any physical attempts to compromise the security functions of the TOE. This policy is addressed by the **O.TOE_INTEGRITY** objective which states that the TOE must provide the means for determining the loss of TOE integrity which could compromise critical security parameters.

P.CONNECT requires that the TOE security policy configured by the Network Manager determines whether networks connected to the TOE are trusted or untrusted, identifies which packet flows are to be protected by the TOE, and relates each protected packet flow with a peer TOE that will decrypt/encrypt the flow. This policy is addressed by the **O.SECURE_PATH** objective which states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE will be able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication. It is also addressed by the **O.ADMIN** objective which states that the TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality in a secure manner.

7.1.2 Security Requirements Rationale

This section demonstrates that the set of security requirements is suitable to meet the set of security objectives and is traceable to the set of security objectives.

Table 7.2: Security Requirements Rationale

Function	O.ANTI_REPLAY	O.INTEGRITY	O.CONFIDENTIALITY	O.DATA_ORIGIN	O.SECURE_PATH	O.ADMIN	O.TOE_INTEGRITY
FAU_ADG.1						X	
FAU_SAR.1						X	
FAU_SAR.2						X	
FCO_NRO.2				X			
FCS_CKM.1			X				
FCS_CKM.4			X				
FCS_COP.1		X	X	X			
FDP_IFC.1					X		
FDP_IFF.1	X	X	X	X	X		
FDP_UCT.1			X				
FDP_UIT.1	X	X					
FIA_UAU.2						X	
FIA_UID.2						X	
FMT_MSA.1					X	X	
FMT_MSA.3					X	X	
FMT_MTD.1 [16]						X	
FMT_MTD.1[17]						X	

[16] Passwords
[17] Unsuccessful login attempts

Function	O.ANTI_REPLAY	O.INTEGRITY	O.CONFIDENTIALITY	O.DATA_ORIGIN	O.SECURE_PATH	O.ADMIN	O.TOE_INTEGRITY
FMT_SMF.1						X	
FMT_SMR. 2						X	
FPT_STM.1						X	
FPT_AMT.1							X
FPT_PHP.1							X
FPT_RVM.1							X
FPT_SEP.1							X
FTA_TSE.1					X		
FTP_ITC.1			X				

The following paragraphs demonstrate that the identified security requirements are appropriate to meet the security objectives.

O.ANTI_REPLAY- The TOE must provide mechanisms to detect that an IP packet flow transmitted to the TOE has not been reused or replayed to establish a TOE session illegally. This objective is satisfied by the following SFRs:

- **FPD_IFF.1 –** This SFR is used to determine the scope and set the parameters for the information flow control policy. Authentication methods, IPSec phase 1 and 2 parameters which include hash and cipher algorithms are part of this SFR. Packets which are not authenticated are discarded and not delivered to the intended receiver.

- **FDP_UIT.1** – This SFR specifies that the TSF must be able to determine on receipt of an IP packet flow whether modification, insertion or replay has occurred. The TOE security policy uses SHA-1. In conjunction with the SHA-1 algorithm, IPSec produces a cryptographic checksum (SHA-1 HMAC) for each packet. Once the HMAC is computed, any subsequent change to the original data will cause a change in the HMAC, and the signature will fail to verify, thus indicating modification of the packet. Additionally, all authenticated communication includes a sequence number which will detect replay.

O.INTEGRITY - The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet flow transmitted to/from the TOE will be detected. This objective is satisfied by the following SFRs:

- **FCS_COP.1** – This SFR specifies that the TOE will perform cryptographic functions using algorithms which meet approved standards. This SFR will ensure that the O.INTEGRITY objective is met, specifically by using the SHA-1 algorithm.

- **FDP_IFF.1 –** This SFR is used to determine the scope and set the parameters for the information flow control policy which serve to define under what conditions information is allowed to flow. IPSec phase 1 and 2 parameters are part of this SFR which include cipher algorithms.

- **FDP_UIT.1** – This SFR specifies that the TSF must be able to determine on receipt of an IP packet flow whether modification, insertion or replay has occurred. The TOE security policy uses SHA-1 for its hash algorithm and the ESP IPSec protocol. In conjunction with the SHA-1 algorithm, IPSec produces a cryptographic checksum (SHA-1 HMAC) for each packet. Once the HMAC is computed, any subsequent change to the original data will cause a change in the HMAC, and the signature will fail to verify, thus indicating modification of the packet.

O.CONFIDENTIALITY - The TOE must provide mechanisms to ensure that IP packets transmitted to/from the TOE over an untrusted network are not made available or disclosed to unauthorized individuals. This objective is satisfied by the following SFRs:

- **FCS_CKM.1 -** This SFR specifies that the TOE will generate cryptographic keys in accordance with a specified algorithm and key size. The generated key will be used for encryption which provides the confidentiality service.

- **FCS_CKM.4 –** This SFR specifies that the TOE will destroy cryptographic keys. This SFR supports the O.CONFIDENTIALITY objective by ensuring that the keys are destroyed once the SA has expired and therefore cannot be compromised.

- **FCS_COP.1** - This SFR specifies that the TOE will perform cryptographic functions using algorithms which meet approved standards. This SFR will ensure that the O.CONFIDENTIALITY objective is met, specifically by using the AES algorithm for encryption and decryption.

- **FDP_IFF.1 –** This SFR is used to determine the scope and set the parameters for the information flow control policy which serve to define under what conditions information is allowed to flow. IPSec phase 1 and 2 parameters are part of this SFR which include cipher algorithms.

- **FDP_UCT.1 -** This SFR specifies that the information flow control policy will be able to transmit and receive objects in a manner protected from unauthorized disclosure.

- **FTP_ITC.1** – This SFR specifies a secure communication channel between the TOE and the remote trusted IT products.

O. DATA_ORIGIN states that the TOE must provide the means for ensuring that an IP packet has been received from a trusted entity. This objective is satisfied by the following SFRs:

- **FCO_NRO.2** - A cryptographic checksum (SHA-1 HMAC) is generated for each IPSec packet. The cryptographic checksum ensures that only computers (sending and receiving) that have knowledge of the keys could have sent the packet. In conjunction with SHA-1 IPSec produces a unique and unforgeable identifier for each packet. Packets which are not authenticated are discarded immediately and are not delivered to the intended recipient.

- **FCS_COP.1 -** This SFR specifies that the TOE will perform cryptographic functions using algorithms which meet approved standards. The TOE implements data origin services for the IP packet by implementing the SHA-1 hash algorithm to create a cryptographic checksum. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys could have sent each packet.

- **FDP_IFF.1 –** This SFR is used to determine the scope and set the parameters for the information flow control policy, which serves to define under what conditions information is allowed to flow. Authentication methods, IPSec Phase 1 and 2 parameters, which include hash and cipher algorithms, are part of this SFR.

O.SECURE_PATH states that the trusted and trained Network Manager responsible for the configuration and administration of the TOE is able to configure a policy that specifies TOE connectivity, packets to be encrypted and packets passed in the clear. The parameters included in this policy will enable the TOE to provide an IPSec channel compliant with RFC 2401, 2408 and 2409 for secure communication. The following SFRs address this objective.

- **FDP_IFC.1** - This SFR requires an information flow control policy which is based on specific attributes. An information flow control policy is enforced between two communicating IPSec peers via the IKE protocol. The identity of the peer IP gateway is assured through the IKE standard which establishes a method for creating security associations and key exchange decisions. Phase 1 of IKE establishes a secure authenticated channel between the communicating CipherOptics SGx appliances with assured identification of end-points.

- **FDP_IFF.1**- This SFR is used to determine the scope and set the parameters for the information flow control policy. Authentication methods, IPSec phase 1 and 2 parameters

which include hash and cipher algorithms are part of this SFR. Packets which are not authenticated are discarded and not delivered to the intended receiver.

- **FMT_MSA.1 –** This SFR ensures that only the Network Manager can change, query, modify and delete the configuration of the security attributes which define the TOE security policy.

- **FMT_MSA.3** – This SFR ensures that the information flow control policy default security parameters are restrictive in nature and that only the Network Manager has the ability to override the initial default settings.

- **FTA_TSE.1** – This SFR ensures that the TOE will deny any attempts to establish a TOE session that has not been specified in the TOE security policy. The TOE security policy includes combination of source/destination IP addresses.

O.ADMIN states that the TOE must provide functionality which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality in a secure manner. This objective is satisfied by the following SFRs:

- **FAU_ADG.1-** This SFR requires that the TOE be able to generate an audit record of auditable events. The TOE monitors successful and unsuccessful login attempts, log outs and records this information in an audit log.

- **FAU_SAR.1 –** This SFR provides the Network Manager with the capability to read all the information recorded in the audit log. It also ensures that the audit records are recorded in a manner suitable for the Network Manager to interpret. The audit log reconstructs an exact sequence of network events or device operations.

- **FAU_SAR.2 –** This SFR ensures that only the Network Manager has access to the audit files.

- **FIA_UAU.2 –** This SFR requires that users are to be successfully authenticated before any actions are taken on behalf of that user.

- **FIA_UID.2** – This SFR requires that each user identify themselves before allowing any other actions on behalf of that user.

- **FMT_MSA.1 –** This SFR ensures that only the Network Manager can change, query, modify and delete the configuration of the security attributes which define the TOE security policy.

- **FMT_MSA.3** – This SFR ensures that the information flow control policy default security parameters are restrictive in nature and that only the Network Manager has the ability to override the initial default settings.

- **FMT_MTD.1**[18] – This SFR ensures that only the Administrator has the ability to modify passwords.

- **FMT_MTD**.**1**[19] – This SFR ensures that only the Administrator has the ability to query, modify and clear the configuration of permitted unsuccessful login attempts.

- **FMT_SMF.1** – This SFR specifies the security functions provided to the Administrator and the Network Manager.

- **FMT_SMR. 2.1** – This SFR requires that both an Administrator and Network Manager role are supported.

- **FMT _SMR.2.2** - This SFR requires that users are associated with roles.

- **FMT_SMR. 2.3** – This SFR ensures that conditions are present which require that users are authenticated before they can be allowed to assume their role.

- **FPT_STM.1 –** This SFR ensures that the TOE can provide reliable time stamps, which will record the timing of security relevant events contained in the audit log.

O.TOE_INTEGRITY states The TOE must provide the means for determining the loss of TOE integrity which could compromise critical security parameters. This objective is satisfied by the following SFRs:

- **FPT_AMT.1 –**This SFR requires that the TOE run a suite of tests during initial start-up to demonstrate the correct operation of the security functions provided by the abstract machine.

- **FPT_RVM.1** – This SFR meets the objective by requiring that the TOE provide the means to ensure that security policy enforcement is not bypassed.

- **FPT_SEP.1** – This SFR meets the objective by requiring that the TOE security functions are provided in a separate operating space that is not accessible by untrusted subjects.

- **FPT_PHP.1** – This SFR requires that TOE provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[18] passwords
[19] unsuccessful login attempts

7.2 TOE Summary Specification Rationale

The table below demonstrates that the correspondence between the TOE SFRs and the summary specification of the TSF. All security functional requirements are addressed by at least one TSF, and the need for each TSF can be attributed to at least one SFR. Detailed descriptions of the TSFs can be found in Section 6.1.

Table 7.3: Summary of Correspondence Between the TSF and SFRs

SFRs	ITSF_ANTI REPLAY	ITSF_INTEGRIYT	ITSF_CONFIDENTIALITY	ITSF_DATA ORIGN	ITSF_SECURE PATH	ITSF_ADMIN	ITSF_TOE INTEGRITY
FAU_ADG.1[20]						X	
FAU_SAR.1						X	
FAU_SAR.2						X	
FCO_NRO.2				X			
FCS_CKM.1			X				
FCS_CKM.4			X				
FCS_COP.1			X	X			
FDP_IFC.1					X		
FDP_IFF.1				X	X		
FDP_UCT.1			X				
FDP_UIT.1	X	X					
FIA_UAU.2						X	
FIA_UID.2						X	
FMT_MSA.1						X	
FMT_MSA.3						X	
FMT_MTD.1[21]						X	

[20] Extended SFR
[21] Passwords

SFRs	ITSF_ANTI REPLAY	ITSF_INTEGRIYT	ITSF_CONFIDENTIALITY	ITSF_DATA ORIGN	ITSF_SECURE PATH	ITSF_ADMIN	ITSF_TOE INTEGRITY
FMT_MTD.1[22]						X	
FMT_SMF.1						X	
FMT_SMR. 2						X	
FPT_STM.1						X	
FPT_AMT.1							X
FPT_PHP.1							X
FPT_RVM.1							X
FPT_SEP.1							X
FTA_TSE.1					X		
FTP_ITC.1			X				

7.2.1 IT Security Functions Rationale (SFRs)

The following table provides a coverage mapping to describe how the TOE Security Functions cover the SFRs.

Table 7.4: TOE Security Functions Rationale

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
FAU_ADG.1	ITSF_ADMIN	It is required that the TOE generates an audit record of specific events and record within each audit record specific details. This is covered in the audit functionality of the TOE which records log file contents in a file and/or on the terminal.

[22] Unsuccessful login attempts

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
FAU_SAR.1	ITSF_ADMIN	It is required that the Network Manager be able to read all the audit information from the audit record and that the audit records are provided in a manner suitable to interpret the information. ITSF_ADMIN details that the TOE records log file contents in a file and/or on the terminal.
FAU_SAR.2	ITSF_ADMIN	It is required that viewing of the log file be restricted to users that have been granted explicit access. ITSF_ADMIN provides the Network Manager with such access.
FCO_NRO.2	ITSF_DATA ORIGIN	It is required that the generation of evidence of origin for transmitted IP data packets is enforced at all times. The TOE implements ESP as the IPSec security protocol which provides data origin authentication. The TOE provides data origin authentication for the communicating TOEs by utilizing x.509 Version 3 certificates. The TOE implements data origin services for the IP packet by implementing the SHA-1 hash algorithm to create a cryptographic checksum. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys could have sent each packet.
FCS_CKM.1	ITSF_CONFIDENTIALITY	It is required that the TOE generate cryptographic keys. The TOE generates cryptographic keys to provide confidentiality services in accordance with the AES algorithm.
FCS_CKM.4	ITSF_CONFIDENTIALITY	It is required that the TOE destroys cryptographic keys. TOE session keys are destroyed after the SA lifetime has expired.
FCS_COP.1	ITSF_CONFIDENTIALITY ITSF_DATA ORIGIN	It is required that the TOE performs encryption, decryption, message signing and key generation. The TOE implements ESP as the IPSec security protocol which provides confidentiality (encryption/decryption), integrity, data origin authentication (message signing) and anti-replay services. (ITSF_CONFIDENTIALITY) The TOE implements data origin services (message signing) for the IP packet by implementing the SHA-1 hash algorithm to create a cryptographic checksum. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		could have sent each packet. (ITSF_DATA_ORGIN) The TOE generates cryptographic keys to provide confidentiality services in accordance with the AES algorithm. (ITSF_CONFIDENTIALITY)
FDP_IFC.1	ITSF_SECURE PATH	It is required that the TOE enforces an information flow control SFP. The TOE implements an information flow control policy between two communicating IPSec peers via the IKE protocol. The identity of the peer IP gateway is assured through the IKE standard which establishes a method for creating security associations and key exchange decisions. Phase 1 of IKE establishes a secure authenticated channel between the communicating CipherOptics SGx appliances with assured identification of end-points. Traffic from one gateway destined to another will only be forwarded if the connection requests and traffic satisfy the information flow policies (SA) configured in the CipherOptics SGx by the Network Manager. If data received by a CipherOptics SGx does not conform to the policy (SA) it will be discarded immediately.
FDP_IFF.1	ITSF_DATA ORIGIN ITSF_SECURE PATH	It is required that the TOE enforces the information flow control SFP based on assigned subject and information security attributes. The TOE implements IPSec which uses IP packet filtering methodology as the basis for determining whether communication is allowed, secured, or blocked. The Network Manager defines the range of traffic to encrypt which is incorporated in the security policy. The TOE implements an information flow control policy between two communicating IPSec peers via the IKE protocol. The identity of the peer IP gateway is assured through the IKE standard which establishes a method for creating security associations and key exchange decisions. Phase 1 of IKE establishes a secure authenticated channel between the communicating CipherOptics SGx appliances with assured identification of end-points. The TOE implements the IPSec protocol that supports two modes of operation (transport and tunnel mode). The CipherOptics SGx supports tunnel mode that protects the entire IP packet including the IP header. When IPSec tunnel mode is used, IPSec encrypts the IP header and the payload. Tunnel mode provides the

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		protection of the entire IP packet by treating it as an ESP payload. The entire IP packet is encapsulated with an ESP header and an additional IP header. The IP addresses of the encapsulated IP header are the ultimate source and destination addresses. The encapsulated portion of the packet indicates where the packet has been signed for integrity and authentication. The encrypted portion of the packet indicates what information is protected with confidentiality. Traffic from one gateway destined to another will only be forwarded if the connection requests and traffic satisfy the information flow policies (SA) configured in the CipherOptics SGx by the Network Manager. If data received by a CipherOptics SGx does not conform to the policy (SA) it will be discarded immediately.
FDP_UCT.1	ITSF_CONFIDENTIALITY	It is required that the TOE provide basic data exchange confidentiality. The TOE implements ESP as the IPSec security protocol which provides confidentiality, integrity, data origin authentication and anti-replay services. The TOE provides confidentiality services by implementing the AES cipher.
FDP_UIT.1	ITSF_INTEGRITY ITSF_ANTI REPLAY	It is required that the TOE provide data exchange integrity. The TOE implements ESP as the IPSec security protocol which provides confidentiality, integrity, data origin authentication and anti-replay services. The TOE provides integrity services by implementing SHA-1. The TOE applies security to IP layer traffic as described in RFC-2401, 2408 and 2409 for secure communication. IPSec allows the exchange and verification of identities without exposing that information to interpretation by an attacker. Mutual verification (authentication) is used to establish trust between the communicating systems and only trusted systems can communicate with each other. After identities are established, IPSec uses cryptography-based keys, shared only by the sending and receiving computers, to create a cryptographic checksum (SHA-1 HMAC) for each IP packet. The cryptographic checksum (SHA-1 HMAC) ensures that only the computers that have knowledge of the keys could have sent each packet. Additionally, all authenticated communication includes a sequence number which will detect replay.

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
FIA_UAU.2	ITSF_ADMIN	It is required that the users (Administrator and Network Manger) are authenticated before any action to take place. The TOE requires the Administrator and Network Manager to enter a correct username and password before allowing any action to take place.
FIA_UID.2	ITSF_ADMIN	It is required that the users (Administrator and Network Manger) are identified before allowing any action to take place. The TOE requires the Administrator and Network Manager to enter a correct username and password before allowing any action to take place.
FMT_MSA.1	ITSF_ADMIN	It is required that the management of security attributes is restricted to authorized users (Network Manager). The Network Manager is responsible for configuring the TOE and its security policies to secure the data and management paths. The restrictive default values as defined for the secure mode configuration ensure that only secure values are accepted for security attributes. The security attributes referenced here refer to key algorithms, modes and lengths. The Network Manager is the only operator with the capability to change the value of the security attributes.
FMT_MSA.3	ITSF_ADMIN	The restrictive default values as defined for the secure mode configuration ensure that only secure values are accepted for security attributes. The security attributes referenced here refer to key algorithms, modes and lengths. The Network Manager is the only operator with the capability to change the value of the security attributes.
FMT_MTD.1[23]	ITSF_ADMIN	It is required that the TOE provide functionality to manage the TSF data. The Administrator is responsible and is provided the functionality for configuring the TOE password.
FMT_MTD.1[24]	ITSF_ADMIN	It is required that the TOE provide functionality to manage the TSF data. The Administrator is responsible and is provided the functionality for configuring unsuccessful login attempt

[23] Passwords

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		functions.
FMT_SMF.1	ITSF_ADMIN	It is required that the TOE provide functionality to manage the TSF. The Administrator is provided the capability to manage passwords and unsuccessful login attempts. The Network Manager is provided the capability to manage the security policies.
FMT_SMR. 2	ITSF_ADMIN	It is required that the TOE supports two roles (Administrator and Network Manager). The TOE provides two roles for managing its security functions. The Administrator and the Network Manager. The Administrator is responsible for password management functions and limiting unsuccessful login attempts. The Network Manager is responsible for configuring the TOE and its security policies to secure the data and management paths. Default passwords must be changed from their initial values. The administrator logs in first and sets the Administrator and Network Manager's password. The passwords must be at minimum eight characters in length but can be up to forty characters in length. Three failed log in attempts are permitted. The TOE requires the Administrator and Network Manager to enter a correct username and password before allowing any action to take place.
FPT_STM.1	ITSF_ADMIN	It is required that the TOE provide reliable time stamps. The TOE provides reliable timestamps via the appliance's internal real time clock and system clock.
FPT_AMT.1	ITSF_TOE INTEGRITY	It is required that the TOE run a suite of tests to demonstrate the correct operation of the abstract machine. The TOE runs a suite of FIPS 140-2 defined self-tests during initial start-up to demonstrate the correct operation of the security functions provided by the abstract machine.
FPT_PHP.1	ITSF_TOE INTEGRITY	It is required that the TOE provides unambiguous detection of physical tampering. The Network Manager by policy definition is required to check the tamper seal periodically in order to detect

[24] Unsuccessful login attempts

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		any physical attempts to compromise the security functions of the TOE.
FPT_RVM.1	ITSF_TOE INTEGRITY	It is required that the TOE ensures that the TSP functions are invoked and succeed before each function within the TSC is allowed to proceed. The TOE runs a suite of FIPS 140-2 defined self-tests during initial start-up to demonstrate the correct operation of the security functions provided by the abstract machine. If any of the tests fail, the boot process is halted. Therefore, no IPSec Policies are loaded, and the network data interfaces are not enabled. This ensures that the CipherOptics SGx cannot perform any cryptographic operations or output any data.
FPT_SEP.1	ITSF_TOE INTEGRITY	It is required that the TSF maintain a security domain for its own execution. The provided tamper seal protects the TOE's hardware and ensures physical separation. All incoming traffic is scanned by the TOE before being processed, which ensures logical separation. The TOE will preserve a secure state to ensure logical separation is maintained under abnormal conditions.
FTA_TSE.1	ITSF_SECURE PATH	It is required that the TSF shall be able to deny session establishment based on the CipherOptics SGx SA policy. Traffic from one gateway destined to another will only be forwarded if the connection requests and traffic satisfy the information flow policies (SA) configured in the CipherOptics SGx by the Network Manager. If data received by a CipherOptics SGx does not conform to the policy (SA) it will be discarded immediately.
FTP_ITC.1	ITSF_CONFIDENTIALITY	It is required for the communication between the TOE and the trusted remote IT products to be secured. Encryption based protection is provided for the communication channels.

7.3 Assurance Measures Rationale

Table 7-4 demonstrates that the correspondence between the TOE SARs and the assurance measures. It illustrates that all security assurance requirements are addressed by at least one assurance measure, and the need for each assurance measure can be attributed to at least one SAR.

Table 7.5: Assurance Measures Rationale

Assurance Component	Assurance Measure	Rationale
ACM_CAP.2	AM_ACM_CAP	A configuration management system for the development process is used and this is documented indicating that the TOE was developed using this CM system.
ADO_DEL.1	AM_ADO_DEL	Secure delivery procedures are documented.
ADO_IGS.1	AM_ADO_IGS	Installation procedures to securely install the TOE are provided. A secure mode of operation is described to ensure the TOE is operating in secure mode.
ADV_FSP.1	AM_ADV_FSP	A functional specification document is provided that describes each security function in the ST. External interfaces are described along with functional behaviour at these interfaces. Error and exception handling is also described.
ADV_HLD.1	AM_ADV_HLD	A document is provided that describes the TOE functionality in subsystems. Interfaces are also described.
ADV_RCR.1	AM_ADV_RCR	A document is provided that maps the functions in the high level design to the functional specification and from the functional specification to the TOE summary specification.
AGD_ADM.1	AM_AGD_ADM	A user manual is provided that indicates the administrator's role and services.
AGD_USR.1	AM_AGD_USR	A user manual is provided that indicates the user's role and services.
ATE_COV.1	AM_ATE_COV	A coverage document is provided that maps the tests completed during development to the functional requirements in the ST.
ATE_FUN.1	AM_ATE_FUN	A test plan and test cases that test each of the security functions in the ST are provided.

Assurance Component	Assurance Measure	Rationale
ATE_IND.2	AM_ATE_IND	This is provided by the evaluation laboratory.
AVA_SOF.1	AM_AVA_SOF	A document describing the strength of function of passwords used is provided.
AVA_VLA.1	AM_AVA_VLA	A vulnerability assessment is provided that examines the TOE in its environment and indicates how the vulnerabilities are mitigated.

CIPHEROPTICS

ANNEX "A"

GLOSSARY

A.1 Common Criteria Terminology

This section contains only those terms that are used in a specialized way in the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or commonly accepted definitions found in ISO security glossaries or other well-known collections of security terms.

Assets

Information or resources to be protected by the countermeasures of a TOE.

Assignment

The specification of an identified parameter in a component.

Assurance

Grounds for confidence that an entity meets its security objectives.

Attack potential

The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation

The addition of one or more assurance component(s) from ISO 15408 Part 3 to an EAL or assurance package.

Authentication data

Information used to verify the claimed identity of a user.

Authorized user

A user who may, in accordance with the TSP, perform an operation.

Component

The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Dependency

A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Evaluation Assurance Level (EAL)

A package consisting of assurance components from ISO 15408 Part 3 that represents a point on the CC predefined assurance scale.

Extension

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in ISO 15408 Part 3 of the CC.

Human user

Any person who interacts with the TOE.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can be the full or abbreviated name of that user or a pseudonym.

Internal communication channel

A communication channel between separated parts of the TOE.

Internal TOE transfer

Communication of data between separated parts of the TOE.

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organizational Security policies

One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Package

A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Protection Profile (PP)

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Refinement

The addition of details to a component.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret

Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Security attribute

Information associated with subjects, users and/or objects that is used for the enforcement of the TSP.

Security Function (SF)

A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP)

The security policy enforced by an SF.

Security objective

A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

Security Target (ST)

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection

The specification of one or more items from a list in a component.

Strength of Function (SOF)

A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic

A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium

A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high

A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.

Subject

An entity within the TSC that causes operations to be performed.

Target of Evaluation (TOE)

An IT product or system, including its associated administrator and user guidance documentation, that is the subject of an evaluation.

TOE resource

Anything useable or consumable in the TOE.

TOE Security Functions (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

A set of rules that regulates how assets are managed, protected and distributed within a TOE.

TOE security policy model

A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control

Communication of data to entities not under control of the TSF.

Trusted channel

A means by which a TSF and a remote trusted IT product can communicate with the necessary confidence to support the TSP.

Trusted path

A means by which a TSF and device physically separated from the TOE can communicate with the necessary confidence to support the TSP.

TSF data

Data created by and for the TOE, which might affect the operation of the TOE.

TSF Scope of Control (TSC)

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User

Any entity (human user, resident added application, or external IT entity) outside the TOE that interacts with the TOE.

User data

Data created by and for the user, which does not affect the operation of the TSF.

A.2 Terminology

The majority of terms are used either according to their accepted dictionary definitions or according to commonly accepted definitions that may be found in ISO security glossaries or other well-known collections of security terms.

AES

The Advanced Encryption Standard is a symmetric key algorithm.

Authentication Header (AH)

A security protocol that provides authentication. AH is embedded in the data to be protected (a full datagram).

End System

A client or server system with an IP address

ESP Encapsulating Security Payload

A security protocol that provides data confidentiality services and optional authentication and replay-detection services. ESP encapsulates the data to be protected.

Extranet

The interconnection of two or more intranets interconnected with an untrusted network using internetworking devices compliant with the TOE to protect packet flows between the intranets.

Federal Information Processing Standards Publication (FIPS PUB)

FIPS PUBS are Federal Information Processing Standards Publications issued by the National Institute Standards and Technology (NIST). The NIST FIPS PUBS related to cryptographic modules and cryptographic algorithms are issued as the framework for the Cryptographic Module and Validation Program (CMVP).

HMAC

Hashed Message Authentication Code, using keyed message digest functions to authenticate a message. The technique used in IPSEC is defined in RFC 2104.

IKE (Internet Key Exchange)

Negotiates the security association (SA) between two entities and exchanges key material two entities and exchanges key material

Internetworking Device

A device that interconnects two or more network segments and forwards IP traffic between the end systems connected to the attached network segments (e.g. a router or firewall).

Intranet

An organization's internal network, constructed from trusted networks (typically LAN's) interconnected with untrusted networks or network segments using internetworking devices

Network

A single network segment or two or more network segments interconnected by internetworking devices

Network Segment

A single physical segment to which end systems are connected

Packet Flow

A unicast flow of IP packets identified by some combination of source/destination IP address, source/destination TCP/UDP port number, TOS field and input interface.

SA

Security Association

SHA-1 Secure Hash Algorithm

Algorithm that takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest provides security against brute-force collision and inversion attacks. SHA-1 [NIS94c] is a revision to SHA that was published in 1994.

Replay Attack

An attempt by an eavesdropper to capture some portion of a transmission and retransmit it at a later time to gain authorized access to the receiver or to spoof the security functions of the receiver.

User

A human that interacts with the TOE to configure and operate the TOE, i.e., an administrator. End users (clients) do not interact with the TOE.

A.3 Terminology

The following glossary of terms is as defined in the CipherOptics 140-2 Security Policy.

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.

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

Session Key

An encryption or decryption key used to encrypt/decrypt the payload of a designated packet.

TCP

Transmission Control Protocol

Tunnel

Logical IP connection in which all data packets are encrypted

UDP

User Datagram Protocol