Certes Networks, Inc.

CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 0.7

Prepared for:

Certes Networks, Inc.
300 Corporate Center Drive
Moon, PA 15108
United States of America

Phone: +1 412 262 2571
www.certesnetworks.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Certes Networks, Inc. CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware and will hereafter be referred to as the TOE throughout this document. The TOE is a high performance, low latency, multi-layer encryption appliance known as a CEP and web-based management software called the CryptoFlow Net Creator. The CEP provides Ethernet frame encryption for Layer 2 networks, Internet Protocol (IP) packet encryption using IP Security (IPSec) for Layer 3 networks, and data payload encryption for Layer 4 MPLS[1] networks. CryptoFlow Net Creator is used to manage the CEP encryption appliances.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) – Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Certes Networks, Inc. CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware Security Target

[1] MPLS – Multiprotocol Label Switching

ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	January 22, 2019
TOE Reference	Certes Networks, Inc. CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware composed TOE consisting of the following components: • CryptoFlow Net Creator v5.3.8447 • CEP220, CEP250, CEP300, CEP420, and CEP520 • CEP v5.3.0290
FIPS 140-2 Status	Level 1 Validated Cryptographic Modules: See tables 12-15 for certificate numbers

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

The TOE is a suite of components consisting of CEP encryption appliances and CryptoFlow Net Creator central security and policy management software. CryptoFlow Net Creator is a web-based GUI[2] that configures and monitors the CEP encryption appliances, stores and deploys policies (or rules), and provides key management and auditing capabilities. Policies created and distributed by CryptoFlow Net Creator define the actions CEPs take on protected network traffic, either to encrypt and decrypt it, send it in the clear, or drop it. All remote management traffic transmitted between the CryptoFlow Net Creator and CEP encryption appliances is protected via TLS[3]v1.2 sessions.

The CEP encryption appliance provides high-speed processing capabilities to protect data travelling over untrusted networks while in transit between sites. It provides Ethernet frame encryption for Layer 2 networks, IPSec encryption for Layer 3 networks, and data payload encryption for Layer 4 MPLS networks. The CEP220, 250, 300, 420, and 520 encryption appliances offer full-duplex, line rate encryption up to 20 Mbps[4], 20 Mbps, 200 Mbps, 1 Gbps[5], and 10 Gbps speeds, respectively, using the Advanced Encryption Standard (AES) algorithm.

Each CEP encryption appliance has one management port and two data ports. A local data port is used for LAN[6] connections to trusted networks, while a remote data port provides WAN[7] connections over untrusted networks. Unencrypted traffic that originates from a trusted, local network is received on the local data port of the origination CEP. This CEP encrypts the received traffic and sends it out through the remote data port to another CEP via an untrusted network, such as Private WAN. At the receiving CEP, the process is reversed; encrypted traffic is received on the CEP remote data port where it is decrypted and sent out the local data port to the destination. Encryption policies use IP addresses, port numbers, protocol IDs[8], or VLAN[9] tags to identify and

[2] GUI – Graphical User Interface
[3] TLS – Transport Layer Security
[4] Mbps – Megabits per Second
[5] Gbps – Gigabits per Second
[6] LAN – Local-Area network
[7] WAN – Wide Area Network
[8] ID – Identifier
[9] VLAN – Virtual Local Area Network

apply security processing to network traffic. CEPs secure network traffic using 256-bit AES[10]-GCM[11] and AES-CBC[12] for encryption, as well as SHA[13]-2 for message integrity and authentication.

The CEP encryption appliance provides full data encryption for Layer 3 IP networks using standard IPSec packet format while preserving the original IP header. It also provides Layer 4 encryption using a patented scheme that protects the IP payload while preserving the original IP and TCP[14]/UDP[15] headers. This unique capability maintains network transparency while providing strong data protection. By preserving the original header and encrypting only the payload, the CEP encryption appliance protects user data over any IP network. This includes any multi-carrier, load-balanced, or high-availability network. This feature also allows network services, such as Netflow/Jflow, and Class of Service (CoS) based traffic shaping to be maintained throughout the network.

The CEP encryption appliances are managed via a CLI[16] hosted on the appliance itself or via the CryptoFlow Net Creator GUI Server running on a separate Linux based platform. The CEP CLI, accessed via serial port or remote SSH[17], is used for initial setup, troubleshooting, and diagnostic tasks.

The CryptoFlow Net Creator GUI is the primary management interface. It is a web-based application and database server supporting role-based access that is used to provision CEP encryption appliances, define polices, and manage keys and certificates. Policies and key data, used by the CEPs to derive encryption keys, are generated and securely distributed to CEP encryption appliances via a TLS authenticated and encrypted channel, with the option for bilateral certificate-based authentication. CryptoFlow Net Creator offers high availability and the web-based, three-tier architecture scales linearly. CryptoFlow Net Creator also provides SNMP[18] access to host information and has the capability to forward logs to an administrator assigned syslog server and generate email notifications when critical alerts are generated in the system.

The CEPs can be deployed into many network topologies.
Table 2 identifies the network topologies that are supported by the TOE's policies.

Table 2 – CEP Network Topologies

Encryption Policy Type	Layer	Topology
Policies	Layer 3	Hub-and-Spoke Point-to-Point Mesh Multicast
	Layer 2	Mesh

[10] AES – Advanced Encryption Standard
[11] GCM – Galois Counter Mode
[12] CBC – Cipher Block Chaining
[13] SHA – Secure Hash Algorithm
[14] TCP – Transmission Control Protocol
[15] UDP – User Datagram Protocol
[16] CLI – Command Line Interface
[17] SSH – Secure Shell
[18] SNMP – Simple Network Management Protocol

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. This section provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is the CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware, which is a software and hardware TOE. The TOE is a CEP encryption appliance, configured and managed using the CryptoFlow Net Creator custom-written application software. The TOE provides Layer 2 Ethernet frame encryption, Layer 3 IP packet encryption, Layer 4 encryption, encryption keys required for the encryption, and a GUI and CLI for the management of its functionality. All of the security features of the TOE, including the cryptographic algorithms, are implemented in the CryptoFlow Net Creator v5.3 Software and the CEP v5.3 Firmware. No security features of the TOE are implemented in the TOE hardware. In addition, the security features are the same amongst all the TOE CEP encryption appliance models.

The CryptoFlow Net Creator v5.3 software includes a FIPS-140-2 validated cryptographic module (cryptographic library). Also, the TOE CEP encryption appliances themselves are FIPS-140-2 validated and are running the CEP v5.3 Firmware that provides all of the FIPS 140-2 validated cryptographic algorithms for the CEP encryption appliances.

The CEP encryption appliances are the policy enforcement points. Because of this, CEPs are referred to as Certes Enforcement Points. According to the policies received, CEPs can encrypt and decrypt traffic, send traffic in the clear, or drop traffic. A brief description of the encryption processes at Layer 2 and Layer 3 is given below:

Layer 2 Ethernet Frame Encryption:
In Layer 2 policies, the CEP provides encryption services to Ethernet frames by using a VLAN ID as an encryption selector or by encrypting all Ethernet frames received from the trusted network.

Layer 3 IP Packet Encryption:
For Layer 3 IP Packet encryption, the CEPs use the IPSec protocol to provide full data encryption for Layer 3 IP networks. They use the Encapsulating Security Payload (ESP) protocol to preserve the original IP packet header and encrypt just the payload. By doing so, the CEPs can encrypt data over load-balanced, redundant, and resilient networks.

Layer 4 Packet Encryption:
Layer 4 packet encryption is a variant of Layer 3 IP Packet encryption in which the CEPs preserve not just the original IP packet header, but also the original TCP/UDP header. Only the traffic payload beyond the original TCP/UDP header is encrypted. This mode allows visibility of the packet to any network monitoring tools in the network.

Before secured data can be exchanged, a Security Association (SA) must be established between the CEP encryption appliances exchanging the information. An SA identifies what traffic to act on, what kind of security to apply, and the CEP with which the traffic is being exchanged. SAs are created when policies are deployed to the CEPs and can be refreshed during a rekey. Two SAs are established for each connection: one for inbound communication and one for outbound communication.

When sending a packet or frame, the CEP checks its Security Policy Database (SPD)[19] to determine which SA to use. The SA determines the security processing required for the packet or frame. For receiving packets or frames, the CEP examines each packet or frame it receives and decides what actions need to be exercised. The actions include one of the following:

- Clear: Packets or frames that match a clear text policy are passed unencrypted.
- Discard: Packets or frames that match a discard policy are dropped and do not exit the CEP.
- Encrypt/Decrypt: All packets matching this policy are encrypted or decrypted.

Figure 1 shows the details of the deployment configuration of the TOE. The following previously undefined acronym appears in Figure 1:

- NTP – Network Time Protocol

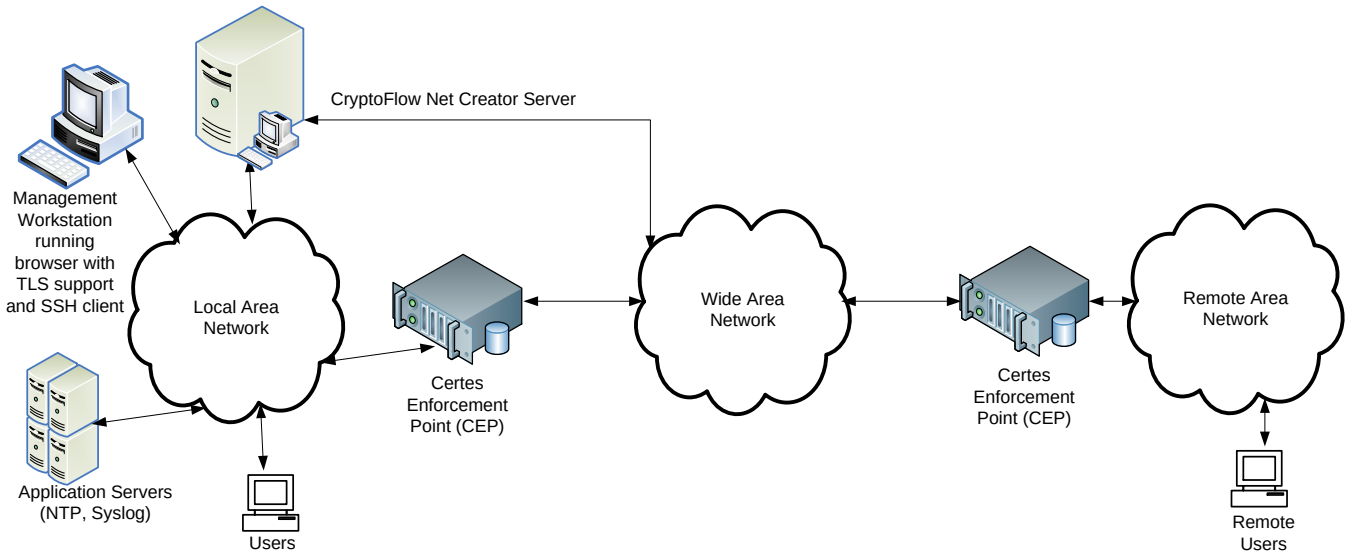

Figure 1 – Deployment Configuration of the TOE

1.4.1 Brief Description of the Components of the TOE

The CEPs can be managed by authorized administrators using the CryptoFlow Net Creator GUI or the CEP CLI. Using the CryptoFlow Net Creator GUI, an administrator can configure and manage multiple appliances from a single centralized location. In addition, security policies defining how and where the encryption will take place can be created. The CEP CLI can be accessed from the management workstation either directly via a serial port or through an SSH connection. It allows an administrator to perform initial setup and troubleshooting of the CEP.

A policy defines networks to be protected and groups these networks to form Network Sets. A policy can have one or more Network Sets associated with it. Once the Network Sets are established, CEPs can be assigned to

[19] SPD – An SPD defines the traffic to be protected, how to protect it, and with whom the protection is shared. The SPD uses selectors to map traffic to a policy, which maps to an SA that is maintained in the Security Association Database (SAD).

those Network Sets and the security policies governing them are defined. Each CEP in a given network is given the same group encryption key data to be used to derive encryption keys. Policy types supported are specified in Table 2. CryptoFlow Net Creator centralizes the creation and distribution of key data and policies. In addition, it provides a rekeying capability that ensures that CEPs generate new encryption keys at defined rekey intervals.

Each policy specifies the encryption and hash algorithms to be used, re-key periods, and whether the key generation technique being used is per Network Set or global. It also specifies the lifetime of the policy, the CEPs that enforce the policy, what kind of traffic the policy acts on, and what actions should be taken on the traffic along with which networks are to be protected. Traffic encryption can be based on the source IP address, destination IP address, source port number, destination port number, protocol ID, or VLAN tag ID.

Once a policy is defined, CryptoFlow Net Creator generates and distributes the required key data and appropriate policies to the CEPs. CryptoFlow Net Creator is installed under a Linux OS[20]. Only the CryptoFlow Net Creator software is included within the TOE boundary, while the physical hardware and Linux OS are considered outside of the TOE boundary.

1.4.2 TOE Environment

The TOE is intended to be deployed in a physically secure cabinet or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms). The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is meant to provide confidentiality and integrity services to information traveling across an untrusted network. The TOE environment should ensure stable network connectivity for the TOE to perform its intended function.

The TOE requires reliable timestamps to audit its security-relevant events. The TOE requires the clocks on the different components of the TOE to be synchronized so that the time each event occurred can be accurately audited. The TOE environment is responsible for providing an NTP server for time synchronization.

The TOE management functionality is accessed via an independent third-party SSH client or Web browser. Any standards-compliant SSH client is suitable for use with the TOE. One of the following types of Web browsers should be used:

- Microsoft Internet Explorer (IE v11+)
- Mozilla Firefox (v64+)
- Google Chrome (v71+)
- Apple Safari (v12+)

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

[20] OS – Operating System

1.5.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE. The TOE is a software and hardware TOE. The TOE is a CEP encryption appliance (both hardware and software) configured and managed using the CryptoFlow Net Creator custom-written application software.

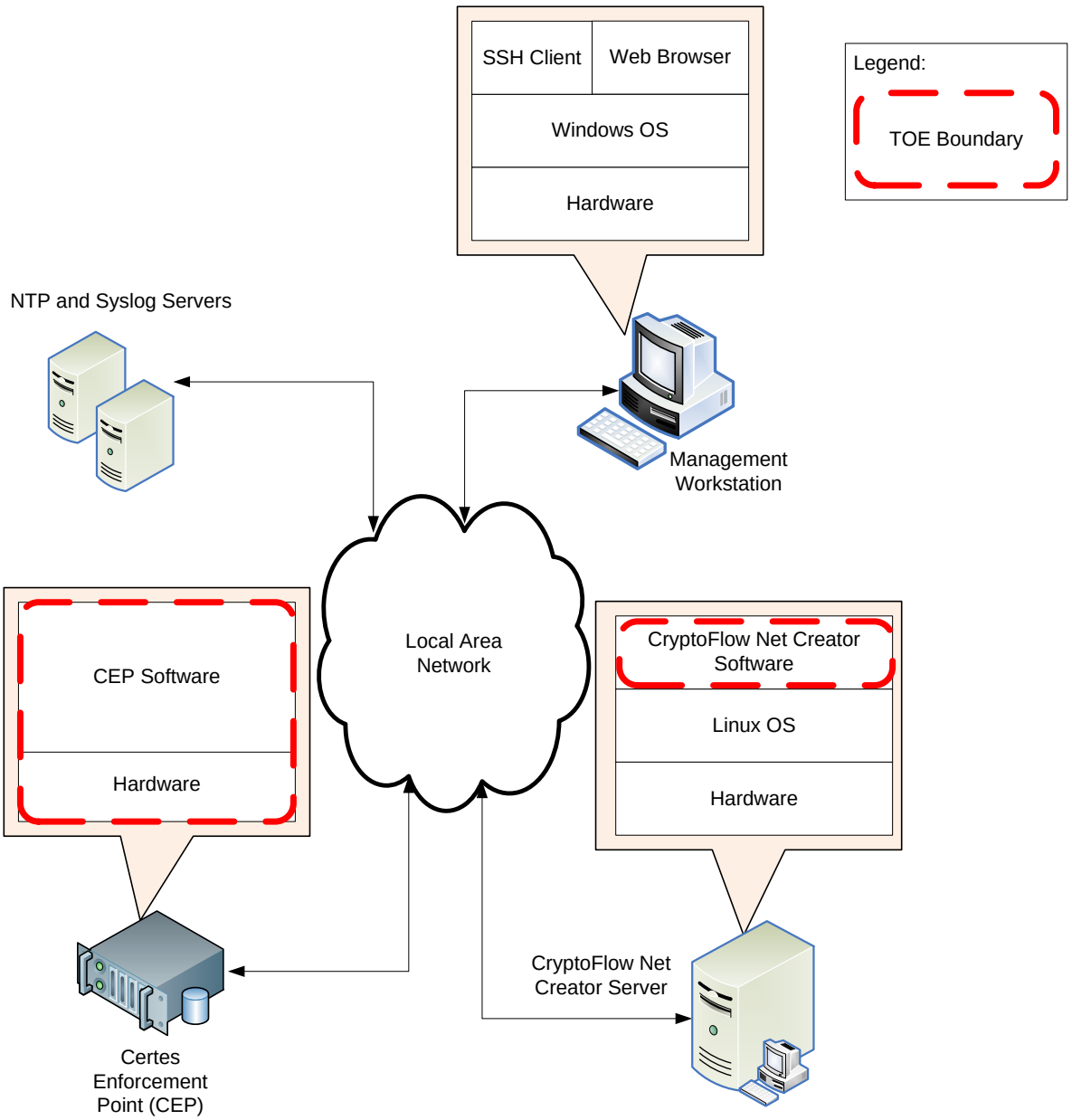

Figure 2 – Physical TOE Boundary

1.5.1.1 TOE Hardware and Software

The essential physical components for the proper operation of the TOE in the evaluated configuration include the following:

- One of each of these Certes encryption appliances:
  - CEP220
  - CEP250
  - CEP300
  - CEP420
  - CEP520
- CryptoFlow Net Creator Server
- CEP v5.3.0290, in binary format pre-installed on the CEP encryption appliances
- CryptoFlow Net Creator v5.3.8447, in binary format pre-installed on the CryptoFlow Net Creator Server

The CryptoFlow Net Creator v5.3.8447 is shipped to customers on a CryptoFlow Net Creator Server that meets the minimum system requirements listed in Table 3.

Table 3 – CryptoFlow Net Creator Server Requirements

Component	Requirement
OS	CentOS 6.7 (with the current released updates applied)
CPU[21]	Intel Xeon E3-1270 v5, 3.6 GHz[22]
Memory	8 GB[23]
Disk Space	500 GB minimum

Only the CEP (hardware and software) and CryptoFlow Net Creator (software-only) are included in the TOE boundary. The CEP hardware includes purpose-built appliances that are included with the purchase of the TOE. The software is custom-made to provide cryptographic functionality and the ability to manage the CEP encryption appliances.

1.5.1.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- *CEP 5.3 User Guide, Version 5.3, REV A*
- *Certes 5.3 Enforcers for Certifications Product Guide, Rev A, 4/20/2018*
- *CFNC User Guide, Version 5.3, REV A*
- *CryptoFlow Net Creator 5.3 Installation Guide, Version 5.3, REV A*

These guides may be downloaded in PDF format from the Certes's Customer Portal at https://support.certesnetworks.com/.

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the Security Function Classes described in the sections below.

[21] CPU – Central Processing Unit
[22] GHz - Gigahertz
[23] GB - Gigabyte

1.5.2.1 Security Audit

The TOE provides functionality for the generation and viewing of audit records. As administrators manage and configure the TOE, the TOE tracks their activities by recording audit records in audit logs. The TOE records all security-relevant configuration settings and changes to ensure accountability of the administrator's actions. Authorized administrators can view the audit records through the CryptoFlow Net Creator GUI and the CEP CLI. The audit records show the identity of the user that triggered the event. The TOE applies a set of rules in monitoring the audited events, and based upon these rules, indicates a potential violation of the enforcement of the SFRs by displaying an alert at the CryptoFlow Net Creator GUI.

1.5.2.2 Cryptographic Support

The TOE uses two FIPS 140-2 validated cryptographic modules to perform cryptographic operations. The cryptographic operations are used to secure communications from remote administrators at the CryptoFlow Net Creator GUI and CEP CLI. They are also used to encrypt user data, create a secure communication channel for the transfer of user data between CEPs, and protect TSF data (e.g., key data, policies) transmitted between CryptoFlow Net Creator and the CEPs. All cryptographic keys generated by the TOE are destroyed by overwriting them according to FIPS 140-2 zeroization methods.

1.5.2.3 User Data Protection

The TOE enforces the Information Flow Control SFP[24] that applies a set of rules to Ethernet frames or IP traffic passing through the TOE. Depending on the operation identified in the SFP, the TOE will determine whether to pass user traffic in the clear, discard it, or encrypt/decrypt it. Authorized TOE administrators configure the SFP by setting security attributes using the CryptoFlow Net Creator GUI or the CEP CLI.

1.5.2.4 Identification and Authentication

All TOE administrators must be identified and authenticated prior to performing any actions at the CryptoFlow Net Creator GUI or CEP CLI. Access to the TOE requires an authorized username and role. This ensures that only legitimate administrators of the TOE can gain access to the configuration and management settings. The TOE obscures passwords at the CryptoFlow Net Creator GUI and CEP CLI during authentication. The CryptoFlow Net Creator GUI uses a bullet (•) in place of each character, and the CEP CLI gives no feedback.

1.5.2.5 Security Management

The TOE is managed by administrators in one of eight roles: Platform Administrator, Administrator, Appliance Administrator, Appliance Operator, Policy Creator, Policy Deployer, User, and Ops. The TOE is capable of performing the following management functions: managing the Information Flow Control SFP security attributes and managing TSF data. The TOE restricts access to management functions based on the administrator's role. The Information Flow Control SFP is permissive by default, allowing information to pass between CEPs in the clear; however, authorized administrators are able to modify the Information Flow Control SFP to perform alternative operations, like dropping or encrypting the information.

1.5.2.6 Protection of the TSF

The TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TOE uses TLSv1.2 to secure communication between CryptoFlow Net Creator and a CEP encryption appliance.

[24] SFP – Security Function Policy

The TOE and TOE environment provide reliable timestamps for the CEP encryption appliance and CryptoFlow Net Creator software, respectively. The timestamps are used to record accurate time for audit records. The time for all TOE components is synchronized using an NTP server in the TOE environment.

1.5.2.7 TOE Access

The TOE terminates an inactive administrator CryptoFlow Net Creator GUI or CEP CLI session after a preconfigured time period. Administrators must re-authenticate after being logged out. This prevents an unauthorized individual from gaining access to the TOE management functions through an unattended session. Administrators may also terminate their own interactive sessions.

Before establishing a user session, the TOE displays a login banner containing an advisory warning message regarding unauthorized use of the TOE.

1.5.2.8 Trusted Path/Channels

The TOE (CEP encryption appliance) provides a trusted channel between itself and another trusted IT[25] product (another CEP encryption appliance in this case) by encrypting and decrypting and authenticating all transmitted data using cryptographic algorithms provided by a FIPS 140-2 validated cryptographic module. It uses this trusted channel to transfer user data (Ethernet frames and IP packets) between CEP encryption appliances.

Using a supported web browser, a remote administrator initiates a secure connection to the CryptoFlow Net Creator GUI. The secure path is established using HTTPS[26]. Using an SSH client, a remote administrator initiates a secure connection to the CEP CLI over SSH. The HTTPS and SSH connections are used to protect data communications from modification or disclosure and ensure end point identification.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

The following features and functionality are not part of the evaluated configuration of the TOE:

- Hardware and Linux OS that CryptoFlow Net Creator runs on
- Strict Authentication
- Non-Transparent Mode
- CryptoFlow Net Creator in High Availability configuration
- SNMP management of CEPs
- Email Alerts

[25] IT – Information Technology
[26] HTTPS – Hyper Text Transfer Protocol Secure

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2018/10/02 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL4+ Augmented with Flaw Remediation (ALC_FLR.3)

3. Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all of the following:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into two categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE (TOE users are, however, assumed not to be willfully hostile to the TOE).

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 5 below lists the applicable threats.

Table 5 – Threats

Name	Description
T.DISCLOSE	An unauthorized person may intercept data within a packet or frame transmitted or received by the TOE when traveling over an untrusted network.
T.MODIFY	An unauthorized person may modify a packet or frame transmitted or received by the TOE when traveling over an untrusted network.
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for them.
T.SPOOF	An unauthorized person may attempt to impersonate the identity (IP address) of a trusted system.
T.UNATH	An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 – Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.
A.TIMESTAMP	The IT environment provides CryptoFlow Net Creator with the necessary reliable timestamps.
A.LOCATE	The TOE, management network, CryptoFlow Net Creator hardware platform, and NTP and syslog servers are all located within a controlled access facility behind a secured network.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.AUDIT	The TOE environment will audit the shutdown of the CryptoFlow Net Creator, which is linked to the shutdown of the CryptoFlow Net Creator audit function.

4. Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.
O.AUDIT	The TOE must record security relevant events with accurate dates and timestamps, associate each event with the identity of the user that caused the event, and provide authorized administrators with the ability to review the audit trail. The TOE shall send an alert email upon detection of potential security violations.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and TSF data.
O.ENCRYPT	The TOE must provide the means of protecting the confidentiality of information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB[27] 140-2.
O.INTEGRITY	The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet or Ethernet frame flow transmitted to or from the TOE will be detected.
O.KEYMAN	The TOE must provide the means for secure management of cryptographic keys. This includes establishment, generation, encryption, and destruction of the keys.
O.PROTECT	The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.
O.SECURE_COMM	The TOE shall securely transfer data between a CEP device and a remote user, CryptoFlow Net Creator, or another CEP device and between CryptoFlow Net Creator and a remote user.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

[27] PUB - Publication

Table 8 – IT Security Objectives

Name	Description
OE.SECURE_NETWORK	The LAN that the CryptoFlow Net Creator hardware platform, CEP, management workstation, and TOE environmental components are connected to a secure network that provides protection against outside attacks.
OE.TRAFFIC	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.TIMESTAMP	NTP servers providing time information to the TOE shall be on the local network and inaccessible to non-administrators.
OE.AUDIT	The TOE environment must audit the shutdown of CryptoFlow Net Creator, which is linked to the CryptoFlow Net Creator audit function.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through the application of procedural or administrative measures.

Table 9 – Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attacks.
OE.TRUSTED_ADMIN	Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

6. Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection, and iteration operations to be performed on security functional requirements. All of these operations are used within this ST with the exception of iteration. These operations are performed as described in Part 2 of the CC and are shown as follows:

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [*underlined text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_ARP.1	Security alarms		✓		
FAU_GEN.1	Audit data generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_SAA.1	Potential violation analysis		✓		
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.2	Cryptographic key agreement		✓	✓	
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_IFC.1	Subset information flow control		✓		

Name	Description	S	A	R	I
FDP_IFF.1	Simple security attributes		✓		
FDP_UCT.1	Basic data exchange confidentiality	✓	✓		
FDP_UIT.1	Data exchange integrity	✓	✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_STM.1	Reliable time stamps			✓	
FTA_SSL.3	TSF-initiated termination		✓		
FTA_SSL.4	User-initiated termination				
FTA_TAB.1	Default TOE access banners				
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		
FTP_TRP.1	Trusted path	✓	✓		

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1

The TSF shall take [*action to make alert viewable via the CryptoFlow Net Creator GUI*] upon detection of a potential security violation.

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;
b. All auditable events, for the [*not specified*] level of audit; and
c. [*other specifically defined auditable events – See Table 11 below*].

FAU_GEN.1.2

The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), 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 PP/ST, [*no other audit relevant information*].

Table 11 – Auditable Events

Component	Auditable Events
CryptoFlow Net Creator	Communication operations and failures with the CEP
	Successful and unsuccessful login attempts, log out activity
	Administrative activity (e.g., modifications to user accounts, appliance configuration changes, and policy deployments)
	CryptoFlow Net Creator output when CryptoFlow Net Creator starts/stops
	Activities regarding updates
CEP	System startup and shutdown, includes reboots and power cycles
	Successful and unsuccessful login attempts and log out activity
	Administrative activities related to CEP user accounts
	Any administrative functions that result in a change to the appliance configuration and data traffic policy deployments
	Appliance software upgrade status
	Failure state entered
	CEP not encrypting

FAU_GEN.2 User identity association

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2.

The TSF shall enforce the following rules for monitoring audited events:

- Accumulation or combination of [*a CEP is not encrypting*] known to indicate a potential security violation;
- [*no other rules*].

FAU_SAR.1 Audit review

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*Platform Administrator, Administrator, Appliance Administrator, Appliance Operator, Policy Creator, Policy Deployer, User, Ops*] 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.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*cryptographic key generation algorithm – see Table 12 and Table 13*] and specified cryptographic key sizes [*cryptographic key sizes – see Table 12 and Table 13*] that meet the following: [*list of standards – see Table 12*].

Table 12 – Cryptographic Key Generation Standards for CryptoFlow Net Creator

Key Generation Type	Key Size	Standards (Certificate #)
AES Key	128, 192, 256	NIST[28] SP[29] 800-133 (5028)
ECDSA Key Pair Gen	P-256, P-384	FIPS PUB[30] 186-4 (1284)
HMAC Key	256, 384, 512	FIPS PUB 198-1 (3342)
Pseudo Random Number Generator	256	NIST SP 800-90A (1842)

Table 13 – Cryptographic Key Generation Standards for CEP

Key Generation Type	Key Size	Standards (Certificate #)
AES Key	128, 192, 256	NIST SP 800-133 (5338)
ECDSA Key Pair Gen	P-224[31], P-256, P-384, P-521	FIPS PUB 186-4 (1402)
HMAC Key	160[32], 256, 384, 512	FIPS PUB 198-1 (3535)
Pseudo Random Number Generator	256	NIST SP 800-90A (2061)

[28] NIST – National Institute of Standards and Technology
[29] SP – Special Publication
[30] PUB – Publication
[31] P-224 used only for pairwise consistency test.
[32] HMAC 160 used only for SNMP, which is outside the scope of the evaluation.

FCS_CKM.2 Cryptographic key agreement (Refinement)

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.2.1

The TSF shall **perform cryptographic key agreement** in accordance with a specified cryptographic key **agreement** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

] ~~that meets the following: [assignment: list of standards]~~.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2 zeroization requirements*].

FCS_COP.1 Cryptographic operation

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform [*cryptographic operations – see Table 14* and *Table 15*] in accordance with a specified cryptographic algorithm [*cryptographic algorithm – see Table 14* and *Table 15*] and cryptographic key sizes [*cryptographic key sizes – see Table 14* and *Table 15*] that meet the following: [*list of standards – see Table 14* and *Table 15*].

Table 14 – Cryptographic Operations of the CryptoFlow Net Creator

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Key Pair Generation and Verification	ECDSA	P-256, P-384	FIPS PUB 186-4 (1284)
Digital Signature Generation and Verification	ECDSA	P-256, P-384	FIPS PUB 186-4 (1284)
Key Agreement	ECC CDH[33] primitive	P-256, P-384	NIST SP 800-56A (1574)
Symmetric Encryption and Decryption	AES (CBC, ECB[34], CCM[35], and GCM mode)	128, 192, 256	FIPS PUB 197 NIST SP 800-38C NIST SP 800-38D (5028)

[33] ECC CDH – Elliptic Curve Cryptography Cofactor Diffie-Hellman

[34] ECB – Electronics Code Book

[35] CCM – Counter with CBC-MAC

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Message Authentication	HMAC-SHA-2	256 384 512	FIPS PUB 198-1 (3342)
Message Digest	SHA-1 SHA-2	160 256 384 512	FIPS PUB 198-1 (4087)
DRBG[36]	AES-CTR[37]	256	NIST SP 800-90A (1842)

Table 15 –Cryptographic Operations of the CEP

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Key Pair Generation and Verification	ECDSA PKG	P-224, P-256, P-384, P-521	FIPS PUB 186-4 (1402)
Digital Signature Generation and Verification	ECDSA SigGen, SigVer	P-224, P-256, P-384, P-521	FIPS PUB 186-4 (1402)
Key Agreement	ECC CDH primitive	P-224, P-256, P-384, P-521	NIST SP 800-56A (1800)
Symmetric Encryption and Decryption	AES (CBC, CFB128 [38], ECB, CMAC[39], and GCM modes)	128, 192, 256	FIPS PUB 197 NIST SP 800-38A NIST SP 800-38D (5338)
Message Authentication	HMAC-SHA-1, HMAC-SHA-2	160 256 384 512	FIPS PUB 198-1 (3535)
Message Digest	SHA-1 SHA-2	160 256 384 512	FIPS PUB 180-4 (4289)
DRBG	AES-CTR	256	NIST SP 800-90A (2061)
Key Derivation, KBKDF[40]	Counter mode with AES-CMAC		NIST SP 800-108 (193)
Key Derivation	TLSv1.2, SSHv2, and SNMPv3		NIST SP 800-135rev1 (1827, 1828, and 1829)

6.2.3 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [*Information Flow Control SFP*] on [

[36] DRBG – Deterministic Random Bit Generator
[37] CTR – Counter
[38] CFB – Cipher Feedback
[39] CMAC – Cipher-based Message Authentication Code
[40] KBKDF – Key-based Key Derivation Function

Subjects: External IT entities[41] that send or receive information through the TOE
Information: Ethernet Frames or IP packets
Operations: Encrypt/decrypt, clear or drop
].

FDP_IFF.1 Simple security attributes

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1

The TSF shall enforce the [*Information Flow Control SFP*] based on the following types of subject and information security attributes:

[

Subject attributes:

1. *Topology*
2. *IP address*

Information attributes:

1. *Source IP Address*
2. *Destination IP Address*
3. *Source port number*
4. *Destination port number*
5. *Protocol ID*
6. *VLAN ID*

].

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*an SA is negotiated and agreed upon for the transmission of Ethernet frames or IP packets*].

FDP_IFF.1.3

The TSF shall enforce the [*no additional information flow control SFP rules*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*none*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*none*].

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies: [FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

[41] In the case of this SFR, trusted external IT entities refers to user workstations sending traffic between CEPs. External IT entities could also refer to traffic originating from another CEP, management workstations used by administrators to manage the TOE, or any other device intended to send traffic to the TOE (switches, routers, NTP servers, etc.).

FDP_UCT.1.1

The TSF shall enforce the [*Information Flow Control SFP*] to be able to [*transmit, receive*] user data in a manner protected from unauthorized disclosure.

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

FDP_UIT.1.1

The TSF shall enforce the [*Information Flow Control SFP*] to be able to [*transmit, receive*] user data in a manner protected from [*modification, insertion*] errors.

FDP_UIT.1.2

The TSF shall be able to determine on receipt of user data, whether [*modification, insertion*] has occurred.

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet [*a defined quality metric* – see *Table 16*].

Table 16 – Password Conventions

Parameters	Conventions
Length	Minimum 8
Case sensitive	Yes
Valid characters	a-z A-Z 0-9 ! @ # % ^ * + = { } : . , _ ~ / \ - [ ]
Spaces allowed	Yes
Dictionary words	Not allowed*
Mix	Must contain at least 2 characters from a mix of upper-case letters, lower case letters, numbers, and non-alphanumeric symbols

*Application Note: Passwords that have a dictionary word are rejected by the CEP. While the CFNC does not reject dictionary words, it mitigates any risk by implementing an administrator-configured limit on the number of allowed failed authentication attempts.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication
FIA_UAU.7.1
The TSF shall provide only [*obscured feedback via CryptoFlow Net Creator GUI and no feedback via CEP CLI*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies
FIA_UID.2.1
The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles
FMT_MSA.1.1
The TSF shall enforce the [*Information Flow Control SFP*] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [*in the policy rules*] to [*Platform Administrator, Administrator, Policy Creator*].

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles
FMT_MSA.3.1
The TSF shall enforce the [*Information Flow Control SFP*] to provide [*permissive*] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2
The TSF shall allow the [*Platform Administrator, Administrator, Policy Creator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles
FMT_MTD.1.1
The TSF shall restrict the ability to [*operations – see Table 17* and *Table 18*] the [*list of TSF data* – see *Table 17* and *Table 18*] to [*the authorized identified roles* – see *Table 17* and *Table 18*].

Table 17 – Management of TSF Data for CryptoFlow Net Creator

Operation	TSF Data	Platform Administrator	Administrator	User	Appliance Admin	Appliance Operator	Policy Creator	Policy Deployer
Modify	Users and Passwords	X	X					
Modify	Password expiration	X	X					
Create, Delete	Users	X	X					
Modify	Usernames and passwords	X	X					
Change	Own password	X	X					
Modify	User's assigned role	X	X					
View	Audit logs and performance statistics	X	X	X	X	X	X	X
Configure	Policies	X	X				X	
Deploy	Policies and keys	X	X					X
Modify	Inactivity timeout interval	X	X					
Configure	Appliances	X	X		X			
View	Appliance statistics	X	X		X	X		

Table 18 – Management of TSF Data for CEP CLI

Operation	TSF Data	Administrator	Ops
Create	Administrator accounts (username and role)	X	
Delete	Administrator accounts	X	
Modify	Administrator's password	X	
Change	Own password	X	X
Modify	Administrator's assigned role	X	
View	Audit logs and performance statistics	X	X[42]
Configure policy mode	CEP policy mode (Layer 2 or Layer 3)	X	
Modify	CLI inactivity timeout interval	X	

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No Dependencies

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of Information Flow Control SFP security attributes, management of TSF data – see Table 17 and Table 18*].

FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

[42] Ops user role can view certain audit logs via the CEP CLI show system-log command but cannot execute the show audit-log command.

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorized identified roles – see Table 19 below*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Table 19 – User Roles

Component	Roles
CryptoFlow Net Creator	Platform Administrator
	Administrator
	Appliance Admin
	Appliance Operator
	Policy Creator
	Policy Deployer
	User
CEP	Administrator
	Ops

6.2.6 Class FPT: Protection of the TSF

FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_ITT.1.1

The TSF shall protect TSF data from [*disclosure, modification*] when it is transmitted between separate parts of the TOE.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_STM.1.1

The TSF shall be able to provide reliable timestamps **for CEP**.

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.3.1

The TSF shall terminate an interactive session after a [*time interval of user inactivity as configured by an administrator*].

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user's own interactive session.

FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TAB.1.1

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

6.2.8 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another 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 [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*transfer of user data between CEPs*].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.

Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, *[HTTPS connections to the CryptoFlow Net Creator GUI, SSH connections to the CEP CLI]*].

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL4 augmented with ALC_FLR.3. Table 20 summarizes these requirements.

Table 20 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims

Assurance Requirements	
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM[43] coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.3 Systematic flaw remediation
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

[43] CM – Configuration Management

7. TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 21 lists the security functionality and their associated SFRs.

Table 21 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.2	Cryptographic key agreement
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
	FDP_UCT.1	Basic data exchange confidentiality
	FDP_UIT.1	Data exchange integrity
Identification and Authentication	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functionality	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_STM.1	Reliable time stamps

TOE Security Functionality	SFR ID	Description
TOE Access	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
	FTA_TAB.1	Default TOE access banners
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generates audit records for start-up and shutdown of the CEP encryption appliance and CryptoFlow Net Creator as well as the events listed in Table 11. These records contain the following information:

- Date and time of the event
- Type of event
- Identity of subject
- Outcome of the event

CEP log files are stored in the CEP file system and can be viewed by authorized administrators from the CEP CLI using the `show audit-log` and `show system-log` commands. CryptoFlow Net Creator audit logs can be viewed by authorized administrators through the **Admin → Audit Log** menu item. CEP logs can also be retrieved (exported from the CEP) and viewed through the CryptoFlow Net Creator GUI. Audit records are displayed in a human-readable format and show the identity of the user that triggered the event.

The TOE applies a set of rules to monitor the audited events and based upon these rules indicates a potential violation of the enforcement of the SFRs by displaying an alert at the CryptoFlow Net Creator GUI. Specifically, the TOE will detect if a CEP is not encrypting.

TOE Security Functional Requirements Satisfied: FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1

7.1.2 Cryptographic Support

The TOE uses two FIPS 140-2 validated cryptographic modules to perform the cryptographic operations listed in Table 14.

The FIPS cryptographic modules are used to provide the following functionality:

- Secure communications from remote administrators to the CryptoFlow Net Creator GUI - relies on the symmetric encryption and decryption operations, HMAC-SHA-2 for message authentication, ECC CDH primitive for key agreement, and ECDSA for digital signatures
- Secure communications from remote administrators to the CEP CLI - relies on the symmetric encryption and decryption operations, HMAC-SHA-2 for message authentication, ECC CDH primitive for key agreement, and ECDSA for the HostKey algorithms
- Data confidentiality of IP packets and Ethernet frames - relies on the symmetric encryption and decryption operations

- Data origin authentication of IP packets and Ethernet frames - relies on HMAC-SHA-2
- Secure communications between CryptoFlow Net Creator and the CEPs using TLSv1.2 - relies on the symmetric encryption and decryption operations, HMAC-SHA-2 for message authentication, ECC CDH primitive for key agreement, and ECDSA for digital signatures
- TOE operator passwords are stored in hashed format using the SHA-512 algorithm
- ECDSA public key is used to authenticate firmware uploads
- SHA-1 is only used in the CRC[44] check of the license string.

The TOE uses the FIPS cryptographic modules to generate the asymmetric and symmetric keys with key sizes as listed in Table 12. The keys are generated by an AES-CTR DRBG, no derivation. The TOE uses an Elliptic curve-based key agreement scheme that meets the following standard: NIST SP 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

All cryptographic keys generated by the TOE are destroyed by overwriting them with zeroes according to FIPS 140-2 zeroization methods. TOE user data encryption keys are destroyed after the SA lifetime has expired.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1.

7.1.3 User Data Protection

The User Data Protection function implements an Information Flow Control policy on user traffic flowing through the TOE. The Information Flow Control SFP enforces rules on subjects that transmit or receive traffic through the TOE. The rules determine what types of operations should be applied to the traffic as the traffic is flowing through the TOE based on the source IP address, destination IP address, source port number, destination port number, protocol ID, and VLAN tag ID.

If the operation in the policy is defined as "encrypt", then the Ethernet frames or IP Packets will be passed with the Ethernet Payload or IP Payload encrypted or decrypted, as appropriate. If the operation in the Policy is defined as "clear", then the Ethernet frames or IP Packets will be passed with the Ethernet Payload or IP Payload without modification. If the operation in the Policy is defined as "drop", then the Ethernet frames or IP Packets will be discarded without further action.

The TOE implements ESP as the IPSec security protocol, which provides confidentiality, integrity, and data origin authentication. The TOE provides confidentiality services by implementing the AES cipher in CBC and GCM mode. The TOE generates cryptographic keys required for encryption in accordance with the AES algorithm. Keys are destroyed after the SA has expired. The TOE provides integrity services by implementing SHA-2. The TOE provides data origin authentication services for the IP packet or Ethernet frame by implementing HMAC-SHA-2. For each packet or frame, this creates a cryptographic checksum ensuring that only the external IT entities (users sending traffic through the CEP) having knowledge of the keys could have sent the packet or the frame.

TOE Security Functional Requirements Satisfied: FDP_IFC.1, FDP_IFF.1, FDP_UCT.1, FDP_UIT.1.

[44] CRC – Cyclic Redundancy Check

7.1.4 Identification and Authentication

The TOE provides functionality that enables authorized administrators to effectively manage the TOE and its security functions.

The TOE requires administrators to enter a correct username and password before allowing any action to take place. The authentication check is intended to prevent an unauthorized person from adding, deleting, or modifying appliance configurations or policies.

In the evaluated configuration, default passwords must be changed from their initial values after the first login. The CryptoFlow Net Creator Platform Administrator logs in first and creates other users, granting them roles and setting their passwords. The CEP Administrator logs in first and sets the Administrator's and Ops passwords. The Platform Administrator and Administrator set their own passwords after their first login. The TOE obscures passwords while authentication is in process using a bullet (•) in place of each character for the CryptoFlow Net Creator GUI and no feedback for the CEP CLI. The password requirements for the TOE are as specified in Table 16.

TOE Security Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.2

7.1.5 Security Management

The Security Management function specifies the management of several aspects of the TSF, including security function behavior and security attributes. The permissions of the administrator roles are also defined in Table 17 and Table 18.

The TOE provides authorized administrators the capability to configure the TOE and its security policies to secure the data and management paths. CryptoFlow Net Creator provides seven administrative roles: Platform Administrator, Administrator, Appliance Admin, Appliance Operator, Policy Creator, Policy Deployer, and User. The TSF maintains a list of permissions for all seven roles. When an administrator logs in and authenticates through the CryptoFlow Net Creator GUI, the TSF shall be able to associate that administrator with one or more of the above roles.

The CEP has two administrative roles: Administrator and Ops. The Administrator role has privileges to manage users, configure the appliance, and create and deploy policies. The Ops role has access to a limited set of CEP CLI commands for initial appliance configuration, status reporting and diagnostics (via `show` commands).

The TOE uses permissive default values for security attributes that are used to enforce the information flow control SFP. The TOE will allow the authorized user to override the default values by specifying alternative initial values.

TOE Security Functional Requirements Satisfied: FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TOE uses TLSv1.2 to secure communication between CryptoFlow Net Creator and a CEP encryption appliance.

The TOE boundary for the CEP includes the hardware and system clock, and therefore the CEP gets the reliable timestamps from the CEP appliance's system clock. The hardware and Linux OS that CryptoFlow Net Creator is installed on is not included in the TOE boundary, and therefore the TOE environment provides the reliable timestamps for CryptoFlow Net Creator.

All the TOE component's times are synchronized with the NTP server. The CEP uses the time from the NTP server to update its system clock used to provide reliable timestamps. The order of the audit records are determined by the value of the timestamps. The time can be synchronized to Coordinated Universal Time manually through the configuration settings. Administrators are assumed to be trusted and competent and may change the system time whenever necessary.

TOE Security Functional Requirements Satisfied: FPT_ITT.1, FPT_STM.1.

7.1.7 TOE Access

The TOE will terminate an administrator CEP CLI or CryptoFlow Net Creator GUI session after an administrator-defined interval of inactivity. Each time a login is completed, the inactivity-timeout value is updated. If the time since the last activity time exceeds the inactivity-timeout value, the administrator is logged out. The `cli inactivity-timer` command sets an inactivity timer for the CEP CLI. The timer applies to a CEP CLI session initiated through the serial port or SSH. Administrators may also terminate their own interactive sessions.

Before establishing a user session, the TOE displays a login banner containing an advisory warning message regarding unauthorized use of the TOE.

TOE Security Functional Requirements Satisfied: FTA_SSL.3, FTA_SSL.4, FTA_TAB.1

7.1.8 Trusted Path/Channels

The trusted path function guarantees a secure channel that the TOE can use to communicate with remote administrators via HTTPS (CryptoFlow Net Creator GUI) and SSH (CEP CLI). The HTTPS and SSH connections are used to protect data communications from modification or disclosure and ensure end point identification.

The TOE provides a trusted channel between CEPs by encrypting and decrypting all transmitted data using cryptographic algorithms provided by a FIPS 140-2 validated cryptographic module. It uses this trusted channel to transfer user data. Only the TOE can initiate this secure channel communication.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.1

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 5.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate that the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 22 below provides a mapping of the objectives to the threats they counter.

Table 22 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DISCLOSE An unauthorized person may intercept data within a packet or frame transmitted or received by the TOE when traveling over an untrusted network.	O.ENCRYPT The TOE must provide the means of protecting the confidentiality of information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB 140-2.	O.ENCRYPT counters this threat by ensuring that information traveling over a public network cannot be intercepted by an un-authorized person. The confidentiality is assured by encryption operations.
	O.KEYMAN The TOE must provide the means for secure management of cryptographic keys. This includes establishment, generation, encryption, and destruction of the keys.	O.KEYMAN counters this threat by ensuring that the cryptographic keys required to provide confidentiality are managed securely, conforming to the standards specified.
	O.SECURE_COMM The TOE shall securely transfer data between a CEP device and a remote user, CryptoFlow Net Creator, or another CEP device and between CryptoFlow Net Creator and a remote user.	O.SECURE_COMM counters this threat by ensuring that data traveling between CEPs is transferred securely.
T.MODIFY An unauthorized person may modify a packet or frame transmitted or received by the TOE when traveling over an untrusted network.	O.INTEGRITY The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet or Ethernet frame flow transmitted to or from the TOE will be detected.	O.INTEGRITY counters this threat by ensuring that the information traveling over a public network cannot be modified by an un-authorized person.
	O.SECURE_COMM The TOE shall securely transfer data between a CEP device and a remote user, CryptoFlow Net Creator, or another CEP device and between CryptoFlow Net Creator and a remote user.	O.SECURE_COMM counters this threat by ensuring that data traveling between CEPs is transferred securely.

Threats	Objectives	Rationale
T.NO_AUDIT An attacker may perform security-relevant operations on the TOE without being held accountable for them.	O.AUDIT The TOE must record security relevant events with accurate dates and timestamps, associate each event with the identity of the user that caused the event, and provide authorized administrators with the ability to review the audit trail. The TOE shall send an alert email upon detection of potential security violations.	O.AUDIT counters this threat by ensuring that security relevant events of the TOE are preserved. O.AUDIT ensures that accurate timestamps are provided for all audit records, allowing the order of events to be preserved.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and TSF data.	O.AUTHENTICATE counters this threat by ensuring that a user or administrator is properly identified, thereby allowing the TSF to record the user's identity for any logs created as a result of the user's or administrator's actions.
	OE.AUDIT The TOE environment must audit the shutdown of CryptoFlow Net Creator, which is linked to the CryptoFlow Net Creator audit function.	OE.AUDIT counters this threat by ensuring that the shutdown of the CryptoFlow Net Creator audit function is captured and preserved by the TOE environment.
T.SPOOF An unauthorized person may attempt to impersonate the identity (IP address) of a trusted system.	O.INTEGRITY The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet or Ethernet frame flow transmitted to or from the TOE will be detected.	O.INTEGRITY counters this threat by guaranteeing the integrity of communications with the TOE. Any attempt to spoof the TOE will be detected by invalid results of integrity checks.
	O.SECURE_COMM The TOE shall securely transfer data between a CEP device and a remote user, CryptoFlow Net Creator, or another CEP device and between CryptoFlow Net Creator and a remote user.	O.SECURE_COMM counters this threat by ensuring that the TOE provides a secure communications channel for use by those attempting to connect to a CEP. Since secure channels are used, any spoofing of CEP components will be indicated by an invalid certificate.
T.UNATH An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	O.ADMIN counters this threat by ensuring that only authorized users have access to TOE management functions.
	O.AUDIT The TOE must record security relevant events with accurate dates and timestamps, associate each event with the identity of the user that caused the event, and provide authorized administrators with the ability to review the audit trail. The TOE shall send an alert email upon detection of potential security violations.	O.AUDIT counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and TSF data.	O.AUTHENTICATE counters this threat by ensuring that users are identified and authenticated prior to gaining access to TOE security data.

Threats	Objectives	Rationale
	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT counters this threat by ensuring that a login banner is displayed regarding unauthorized use of the TOE.

Every threat is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 23 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 23 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.TRUSTED_ADMIN Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.	OE.TRUSTED_ADMIN upholds this assumption by ensuring that the TOE administrators read and follow the guidance for installation and deployment of the TOE.
A.NETCON The TOE environment provides the network connectivity required to allow the TOE to perform its intended functions.	OE.TRAFFIC The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.TRAFFIC upholds this assumption by ensuring that the environment provides the TOE with the appropriate network configuration.
A.TIMESTAMP The IT environment provides CryptoFlow Net Creator with the necessary reliable timestamps.	OE.TIMESTAMP NTP servers providing time information to the TOE shall be on the local network and inaccessible to non-administrators.	OE.TIMESTAMP upholds this assumption by ensuring that NTP servers providing timestamps are on the local network and in-accessible to non-administrators.
A.LOCATE The TOE, management network, CryptoFlow Net Creator hardware platform, and NTP and syslog servers are all located within a controlled access facility behind a secured network.	OE.PHYSICAL Those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attack.	OE.PHYCAL upholds this assumption by ensuring that the environment provides protection against physical attack.
	OE.SECURE_NETWORK The LAN that the CEP, CryptoFlow Net Creator hardware platform, management workstation, and TOE environmental components are connected to is a secure network that provides protection against outside attacks.	OE.SECURE_NETWORK upholds this assumption by ensuring that the TOE and TOE environmental components connected to the LAN are protected from outside attacks.

Assumptions	Objectives	Rationale
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.TRUSTED_ADMIN Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.	OE.TRUSTED_ADMIN upholds this assumption by ensuring that those responsible for the TOE will provide competent individuals to perform management of the security of the environment and restrict these functions and facilities from unauthorized use.
A.NOEVIL The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.	OE.TRUSTED_ADMIN Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.	OE.TRUSTED_ADMIN upholds this assumption by ensuring that all administrators assigned to manage the TOE are not careless, negligent, or willfully hostile; are appropriately trained; and follow all administrator guidance.
A.AUDIT The TOE environment will audit the shutdown of the CryptoFlow Net Creator, which is linked to the shutdown of the CryptoFlow Net Creator audit function.	OE.AUDIT The TOE environment must audit the shutdown of CryptoFlow Net Creator, which is linked to the CryptoFlow Net Creator audit function.	OE.AUDIT upholds this assumption by ensuring that TOE environment audits shutdown of CryptoFlow Net Creator and therefore audits the shutdown of the CryptoFlow Net Creator audit function.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.

Every assumption is mapped to one or more objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended assurance requirements defined for this TOE.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 24 below shows a mapping of the objectives and the SFRs that support them.

Table 24 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	FIA_SOS.1 Verification of secrets	This requirement meets the objective by ensuring that the authentication process meets the password requirements of the TOE.
	FIA_UAU.2 User authentication before any action	This requirement meets the objective by requiring all TOE administrators to authenticate before any other TSF-mediated actions are performed.
	FIA_UID.2 User identification before any action	This requirement meets the objective by requiring all TOE administrators to identify before any other TSF-mediated actions are performed.
	FMT_MSA.1 Management of security attributes	This requirement meets the objective by allowing authorized TOE administrators to manage the TOE security attributes.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MTD.1 Management of TSF data	This requirement meets the objective by ensuring that the TOE restricts access to TSF data based on the user's role.
	FMT_SMF.1 Specification of management functions	This requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	This requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record security relevant events with accurate dates and timestamps, associate each event with the identity of the user that caused the event, and provide authorized administrators with the ability to review the audit trail. The TOE shall send an alert email upon detection of potential security violations.	FAU_ARP.1 Security alarms	The requirement meets this objective by ensuring that the TOE sends email alerts for potential security violations.
	FAU_GEN.1 Audit Data Generation	This requirement meets the objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User Identity Association	The requirement meets the objective by identifying the users that perform functions resulting in audit records.
	FAU_SAA.1 Potential violation analysis	The requirement meets the objective by identifying potential security violations that result in email alerts.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensure that the TOE provides the ability to review logs.

Objective	Requirements Addressing the Objective	Rationale
	FPT_STM.1 Reliable time stamps	This requirement meets the objective by ensuring that the TOE can provide reliable timestamps. The timestamps allow the TOE to place events in the order that they occurred.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and TSF data.	FIA_SOS.1 Verification of secrets	This requirement meets the objective by ensuring that the authentication process meets the password requirements of the TOE.
	FIA_UAU.2 User authentication before any action	This requirement meets the objective by requiring all TOE administrators to authenticate before any other TSF-mediated actions are performed.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring feedback through CryptoFlow Net Creator and the CEP CLI during authentication.
	FIA_UID.2 User identification before any action	This requirement meets the objective by requiring all TOE administrators to identify before any other TSF-mediated actions are performed.
	FMT_MTD.1 Management of TSF data	This requirement meets the objective by ensuring that only authorized users are allowed access to TSF data, including authentication data.
	FTA_SSL.3 TSF-initiated termination	This requirement meets the objective by ensuring that the TOE users are logged off after an administrator-defined period of inactivity, ensuring that unauthenticated entities do not gain access to the TOE through an unattended session. This ensures that unauthenticated users do not hijack an authorized administrator's unattended session.
	FTA_SSL.4 User-initiated termination	This requirement meets the objective by providing a means for TOE users to log off to terminate their sessions, ensuring that unauthenticated entities do not gain access to the TOE through an unattended session. This ensures that unauthenticated users do not hijack an authorized administrator's unattended session.
O.ENCRYPT The TOE must provide the means of protecting the confidentiality of information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB 140-2.	FCS_CKM.1 Cryptographic key generation	This requirement meets the objective by ensuring that the cryptographic keys are generated according to an assigned standard.
	FCS_CKM.2 Cryptographic key agreement	This requirement meets the objective by ensuring that key agreement is performed according to defined standards.
	FCS_CKM.4 Cryptographic key destruction	This requirement meets the objective by ensuring that the cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.

Objective	Requirements Addressing the Objective	Rationale
	FCS_COP.1 Cryptographic operation	This requirement meets the objective by ensuring that the cryptographic operations are performed according to the specified algorithms with the specified key sizes.
	FDP_IFC.1 Subset information flow control	This requirement meets the objective by defining the types of subjects, information, and operations for the Information Flow Control SFP that is applied to traffic flowing through the TOE.
	FDP_IFF.1 Simple security attributes	This requirement meets the objective by defining a list of attributes of subjects and information for the Informational Flow Control SFP that is applied to traffic flowing through the TOE.
	FDP_UCT.1 Basic data exchange confidentiality	This requirement meets the objective by ensuring that the traffic flowing through the TOE is protected from unauthorized disclosure.
	FMT_MSA.3 Static attribute initialisation	This requirement supports the objective by specifying that the Informational Flow Control policy shall be applied permissively to traffic flowing through the TOE. This means that the IP packets or Ethernet frames are sent unencrypted by default. Authorized administrators can modify the default values to ensure that some or all traffic is decrypted instead.
	FTP_ITC.1 Inter-TSF trusted channel	This requirement meets the objective by ensuring that any information exchange between the TOE and another trusted IT product happens over a trusted channel.
O.INTEGRITY The TOE must provide mechanisms to ensure that any attempt to corrupt or modify an IP packet or Ethernet frame flow transmitted to or from the TOE will be detected.	FCS_COP.1 Cryptographic operation	This requirement meets the objective by ensuring that the cryptographic operations are performed according to the specified algorithms with the specified key sizes.
	FDP_UIT.1 Data exchange integrity	This requirement meets the objective by ensuring that the traffic flowing through the TOE is protected from modification and insertion errors.
O.KEYMAN The TOE must provide the means for secure management of cryptographic keys. This includes establishment, generation, encryption, and destruction of the keys.	FCS_CKM.1 Cryptographic key generation	This requirement meets the objective by ensuring that the cryptographic keys are generated according to an assigned standard.
	FCS_CKM.2 Cryptographic key agreement	This requirement meets the objective by ensuring that key agreement is performed according to defined standards.
	FCS_CKM.4 Cryptographic key destruction	This requirement meets the objective by ensuring that the cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.

Objective	Requirements Addressing the Objective	Rationale
	FCS_COP.1 Cryptographic operation	This requirement meets the objective by ensuring that the cryptographic operations are performed according to the specified algorithms with the specified key sizes.
O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	FTA_TAB.1 Default TOE access banners	This requirement meets the objective by displaying an advisory warning message regarding unauthorized use of the TOE.
O.SECURE_COMM The TOE shall securely transfer data between a CEP device and a remote user, CryptoFlow Net Creator, or another CEP device and between CryptoFlow Net Creator and a remote user.	FPT_ITT.1 Basic internal TSF data transfer protection	This requirement meets the objective by ensuring that TSF data transmitted between the CryptoFlow Net Creator and a CEP device or between CEP devices is protected.
	FTP_ITC.1 Inter-TSF trusted channel	This requirement meets the objective by providing a trusted channel for the transfer of user data between CEP devices.
	FTP_TRP.1 Trusted path	This requirement meets the objective by protecting the communication path to remote users of CryptoFlow Net Creator and the CEP CLI.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was chosen because it is best suited to address the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. EAL4+ allows the vendor to evaluate their product at a detailed level while benefitting from the Common Criteria Recognition Agreement. The chosen assurance level is appropriate for the threats defined in the environment. At EAL4+, penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

The augmentation of ALC_FLR.3 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria and SFRs explicitly stated in this ST. Table 25 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 25 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_ARP.1	FAU_SAA.1	✓	
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.2	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FDP_UCT.1	FDP_IFC.1	✓	
	FTP_ITC.1	✓	
FDP_UIT.1	FDP_IFC.1	✓	
	FTP_ITC.1	✓	
FIA_SOS.1	No dependencies	✓	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MSA.1	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1, is included. This satisfies this dependency.
FPT_ITT.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FTA_SSL.3	No dependencies	✓	
FTA_SSL.4	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FTA_TAB.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

9. Acronyms

Table 26 defines the acronyms used throughout this document.

Table 26 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CEP	Certes Enforcement Point
CLI	Command Line Interface
CM	Configuration Management
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CTR	Counter
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GB	Gigabyte
Gbps	Gigabits per second
GHz	Gigahertz
GCM	Galois Counter Mode
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
HTTPS	Hyper Text Transfer Protocol Secure
ID	Identifier
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security Protocol

Acronym	Definition
IT	Information Technology
LAN	Local-Area Network
MAC	Message Authentication Code
Mbps	Megabits per second
MPLS	Multiprotocol Label Switching
NTP	Network Time Protocol
PUB	Publication
OS	Operating System
OSP	Organizational Security Policy
PMTU	Path Maximum Transmission Unit
PP	Protection Profile
RSA	Rivest-Shamir-Adleman
RNG	Random Number Generator
SA	Security Association
SAD	Security Association Database
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SPD	Security Policy Database
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
WAN	Wide Area Network
XML-RPC	Extensible Markup Language Remote Procedure Call

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com