Certes Networks, Inc.

TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware

Security Target

Evaluation Assurance Level (EAL): EAL4+
Document Version: 1.3

Prepared for:

Certes Networks, Inc.

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
United States of America

Phone: +1 877 878 6655
Email: info@certesnetworks.com
http://www.certesnetworks.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Certes TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware, and will hereafter be referred to as the TOE throughout this document. The TOE is a high performance, low latency, bandwidth customizable encryption appliance. It provides Ethernet frame encryption for layer 2 networks, and Internet Protocol (IP) packet encryption for layer 3 networks.

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 functions 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, 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 met by the TOE.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements 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 ST and TOE References

ST Title	Certes Networks, Inc. TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware Security Target
ST Version	Version 1.3
ST Author	Corsec Security, Inc.
ST Publication Date	2012-11-21
TOE Reference	Certes TrustNet Manager Platform v3.4.5543 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running Certes Enforcement Point v2.1.1 Firmware with Software Version Hash: 6a9fdea59ee8a1c17bf9dd8ca78065a3f91d503d

FIPS 140-2 Status	Level 2, Validated crypto module, Certificate Nos. 1797, 1798, and 1799

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.

Certes TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware is a suite of components consisting of Certes Enforcement Point (CEP) (an encryption appliance) and the TrustNet Manager software. TrustNet is a three-tiered web-based application and database server containing the business logic as well as configuration and policy information. TrustNet Manager is accessed through a standard web-browser interface.

The workhorse of the TrustNet Manager Platform suite is the CEP appliance. The appliance provides high-speed processing capabilities to protect data in transit between sites while it travels over untrusted networks. It is a flexible encryption appliance that provides Ethernet frame encryption for Layer 2 networks and IP packet encryption for Layer 3 networks. The CEP 10, 100, 1000, and 10G appliances offer full-duplex, line rate encryption at 10 Mbps[1], 100 Mbps, 1 Gbps[2], and 10 Gbps speeds respectively using the Advanced Encryption Standard (AES) and Triple-Data Encryption Standard (DES) algorithms.

The CEP has two data ports: a local port and a remote port that interface with other network equipment. Unencrypted traffic that originates from a trusted, local network is received on the local port of the origination CEP. This CEP then encrypts the received traffic, and sends it out through the remote port to another CEP via an untrusted network, such as the Internet. At the receiving CEP, the process is reversed; encrypted traffic is received on the CEP remote port and decrypted. Then the decrypted traffic is sent from the local port to the final destination.

TrustNet Manager is the management system that drives the solution. It is a web application and database server that is accessed using a browser-based GUI and supports role-based access. It is through this multi-user web user interface that the CEP devices are configured and policies defined. TrustNet Manager handles the policy generation and distribution. TrustNet Manager offers high availability and the web-based, three-tier architecture scales linearly. TrustNet Manager is responsible for distributing the key material for use by the CEP devices. TrustNet Manager also provides SNMP[3] access to host information, and has the capability to forward logs to an administrator assigned syslog server.

Table 2 below identifies the types of policies that administrators are allowed to create, based on the network topology of the deployment.

[1] Mbps – Megabits per second

[2] Gbps – Gigabits per second

[3] SNMP – Simple Network Management Protocol

Table 2 Policy Types

Policy Type	Layer	Topology
Distributed Key Policies	Layer 3	Hub-and-Spoke Point-to-Point Mesh Multicast
	Layer 2	Mesh
Negotiated IKE[4] Policies	Layer 2	Point-to-Point

1.4 TOE Overview

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

The TOE is the TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware, which is a software and hardware TOE. The TOE is a Certes custom-built hardware encryption appliance, configured and managed using custom-written application software. The TOE provides Layer 2 Ethernet frame encryption and Layer 3 IP packet encryption, encryption keys required for the encryption, and GUIs and Command Line Interfaces (CLI) for the management of its functionality.

CEPs are the policy 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:
During the Ethernet Frame encryption process with the CEPs, each and every Ethernet Frame is authenticated. The CEPs can encrypt data based on the VLAN ID or they can simply encrypt all Ethernet frames.

Layer 3 IP Packet Encryption:
For IP Packet encryption, the CEP uses the IP Security (IPSec) protocol to provide full data encryption for Layer 3 IP networks. It utilizes 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.

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

[4] IKE – Internet Key Exchange

When sending an outbound packet or frame the CEP checks its Security Policy Database (SPD)[5] to determine which SA to use. The SA determines the security processing required for the packet or frame. For inbound packets or frames, the CEP examines each packet or frame it receives and decides on what actions needed 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: Encrypts or decrypts all packets matching this policy.

Figure 1 shows the details of the deployment configuration of the TOE using TrustNet Manager. The policy and status information are exchanged between TrustNet Manager and the CEP.

The following acronyms that have not been previously defined appear in the figure below:

- NTP – Network Time Protocol
- SNMP – Simple Network Management Protocol

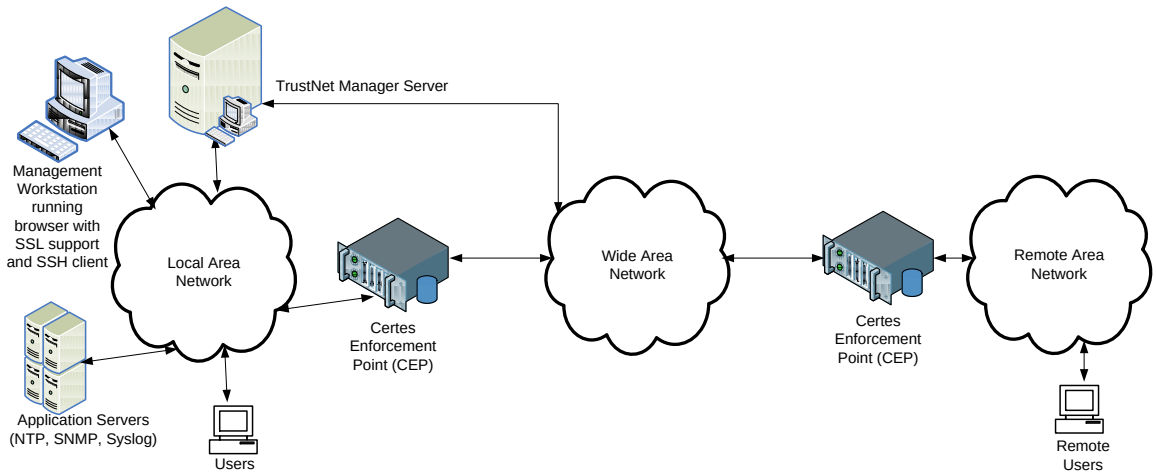

Figure 1 Deployment Configuration of the TOE

The CEP can be managed by authorized administrators via the Web GUI or directly via CLI commands. Through the GUI into TrustNet Manager, 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.

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

[5] 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).

assigned to those Network Sets and the security policies governing them are defined. Each CEP in a given network is given the same encryption key material. Policy types supported are specified in Table 2.

For Distributed Key Policies, TrustNet Manager centralizes the creation and distribution of encryption keys and policies. By doing so, multiple CEPs can use common keys, while the centralized platform performs the function of renewing keys at pre-determined intervals. For Negotiated IKE policies the CEP's can be configured directly via the CLI or using the TrustNet Manager GUI. Keys are negotiated directly without requiring a centralized key generation and distribution tool.

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 source IP[6] address, destination IP address, source port number, destination port number, protocol ID[7], or VLAN[8] tag ID.

Once a policy is defined, TrustNet Manager generates and distributes the required encryption keys to the CEPs along with the appropriate policies. TrustNet Manager can be installed under Linux or can be run inside of a Virtual Machine (VM). In either case, only the TrustNet Manager software is included within the TOE boundary, while the virtual hardware, physical hardware, and Linux OS are considered outside of the TOE boundary.

A CLI allows an administrator to perform initial setup of the CEP. It also facilitates the troubleshooting commands for the CEP. In Layer 2 point-to-point deployments, authorized administrators can also create point-to-point policies using the CLI.

1.4.1 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, etc.). 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 that 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 to provide for this setup.

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. The browser used should be one of:

- Internet Explorer 7 or above,

[6] IP – Internet Protocol
[7] ID – Identifier
[8] VLAN – Virtual Local Area Network

- Firefox 3 or above,
- Chrome, or
- Safari.

1.5 TOE Description

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

1.5.1 Physical Scope

This section will primarily address the physical and logical components of the TOE included in the evaluation. Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the constituents of the TOE Environment.

The TOE is a software and hardware TOE. The TOE is a Certes custom-built hardware encryption appliance, configured and managed using custom-written application software.

Undefined acronyms in the figure below:

- SSH – Secure Shell

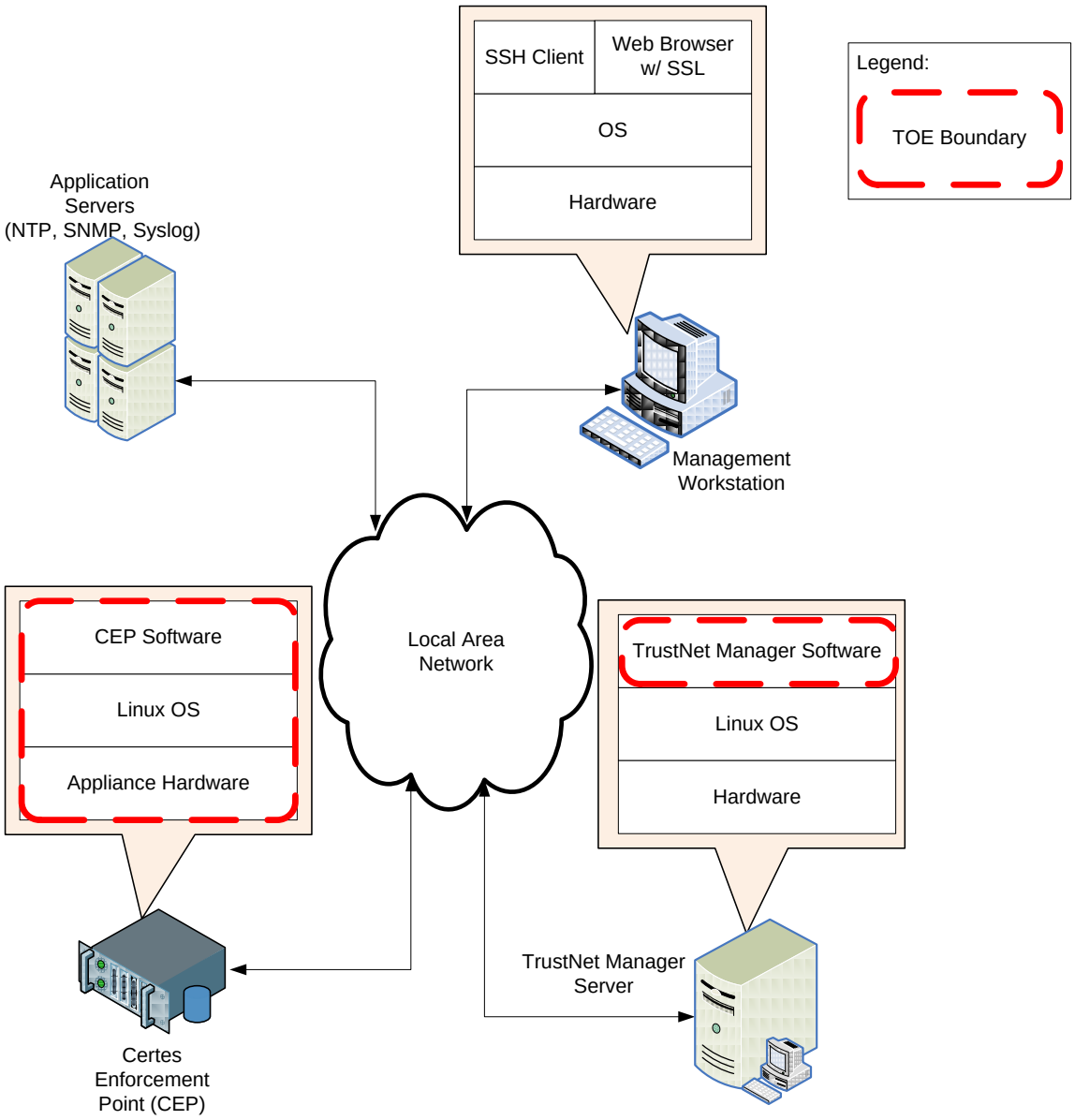

Figure 2 TOE Boundary

1.5.1.1 TOE Hardware and Software

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

- two of the Certes encryption appliances below:
  - CEP10-VSE
  - CEP100-VSE
  - CEP1000-VSE

  - CEP10G-VSE
- the Linux Operating System (OS) running on the CEP Hardware,
- CEP v2.1.1 Software,
- TrustNet Manager v3.4 Software.

The minimum system requirements of the machine on which the TrustNet Manager software is to be installed are listed in Table 3 .

Table 3 TrustNet Manager Platform requirements

Component	Requirement
Operating System	CentOS 6 (with the current released updates applied)
CPU	X86, 32 or 64 bit, Quad Core Recommended
Memory	4GB
Disk Space	100GB Minimum

Only the CEP (hardware and software) and TrustNet Manager (software-only) are included in the TOE boundary. The 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 appliances that provide said functionality.

1.5.1.2 Guidance Documentation

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

- CEP VSE Certes Enforcement Point CLI User Guide Version 2.1.1
- CEP VSE Certes Enforcement Point CLI Installation Guide Version 2.1.1
- CEP VSE Release Note – Version 2.1.1
- TrustNet Manager User Guide Version 3.4
- TrustNet Manager Installation Guide Version 3.4
- TrustNet Manager Release Notes – Version 3.4

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 security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[9]

[9] TSF – TOE Security Functionality

- TOE Access
- Trusted channels

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, sort, and filter the audit records.

1.5.2.2 Cryptographic Support

The TOE provides for the secure communication of management and user data. The CEP facilitates this by employing cryptographic operations and establishing a secure channel. The secure channel is used for management sessions between a CEP device and a remote workstation and also with another CEP device for passing user data. The secure channel allows the CEP to pass sensitive information while addressing the threats of unauthorized disclosure and modification. A Federal Information Processing Standard (FIPS) 140-2 validated cryptographic module performs all CEP related cryptographic operations.

1.5.2.3 User Data Protection

The User Data Protection function implements functionality necessary to protect user data which is entrusted to the TOE. Access to the management functions is partitioned according to the administrator's role. The TOE enforces an information flow control SFP[10] that applies a set of rules to Ethernet or IP traffic passing through the TOE. Depending on the operation identified in the security policy, the TOE will determine whether to pass user traffic in the clear, discard it, or apply encryption to it.

1.5.2.4 Identification and Authentication

The TOE identifies and authenticates each operator of the TOE. 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.

1.5.2.5 Security Management

The Security Management functionality of the TOE specifies several aspects of management of the TSF. The TOE management functionality includes defining the security function behavior, and its associated security attributes. The Security Management function specifies the roles defined for managing the TOE and how administrators assume the roles, as well as defining who is allowed to manage the TSF data.

1.5.2.6 Protection of the TSF

The TOE provides reliable time stamps for the CEP appliance, and TOE Environment provides time stamps for the TrustNet Manager software components, that it will use to record the accurate time for audit records. The different components of the TOE time are synchronized with an NTP server.

1.5.2.7 TOE Access

The TOE terminates an inactive administrator CLI session or TrustNet Manager 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. User sessions are also terminated after a configurable period of inactivity.

---

[10] SFP – Security Functional Policy

1.5.2.8 Trusted channels

The Trusted Channels function establishes a secure communication channel between the CEP and a trusted external IT[11] entity. Encryption-based protection is provided to establish a secure channel.

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

Features/Functionality that are not part of the TOE are:

- the hardware and Linux OS that TrustNet Manager runs on
- Configuring TrustNet Manager for High Availability
- SNMP Management of CEPs
- CEPs in Non-Transparent mode (Transparent Mode disabled)

[11] IT – Information Technology

2 Conformance Claims

This section provides the identification for any CC, Protection Profile (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, Revision 3, July 2009; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2011/03/01 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:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with 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. The following threats are applicable.

Table 5 Threats

Name	Description
T.NO_AUDIT	An attacker may perform security-relevant operations on the TOE without being held accountable for it.
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.UNATH	An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration.
T.SPOOF	An unauthorized person may attempt to impersonate the identity (IP address) of a trusted system.

3.2 Organizational Security Policies

There are no Organizational Security Policies (OSPs) for this ST.

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. The following specific conditions 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 TrustNet Manager with the necessary reliable timestamps.
A.LOCATE	The connection between the CEP and TNM, management workstation which is connected to TNM, and TOE Environmental components (the NTP, SNMP, and syslog servers) are all located within a controlled access facility behind on a secured network.
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.

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 as follows:

Table 7 Security Objectives for the TOE

Name	Description
O.AUDIT	The TOE must record events of security relevance with accurate dates and timestamps. The TOE must provide the authorized administrators with the ability to review the audit records.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its security functions, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.KEYMAN	The TOE must provide the means for secure management of cryptographic keys. This includes generation, encryption and destruction of the keys.
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.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.SECURE_COMM	The TOE shall securely transfer data between a CEP device and management workstation and a CEP device and another CEP device.

4.2 Security Objectives for the Operational Environment

4.2.1 IT Security Objectives

The following IT security objectives are to be satisfied by the environment.

Table 8 IT Security Objectives

Name	Description
OE.SECURE_NETWORK	The Local Area Network that the CEP and TNM, and Management workstation used for TNM, and TOE environmental components are connected to is 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.

4.2.2 Non-IT Security Objectives

The following non-IT environment security objectives 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 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 attack.
OE.TRUSTED_ADMIN	Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.

5 Extended Components

There are no extended SFRs and extended SARs for this TOE.

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. 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_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
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	✓	✓		
FIA_SOS.1	Verification of secrets		✓		

Name	Description	S	A	R	I
FIA_UAU.2	User authentication before any action				
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_STM.1	Reliable Time Stamps			✓	
FTA_SSL.3	TSF-initiated termination		✓		
FTP_ITC.1	Inter-TSF trusted channel	✓	✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation
Hierarchical to: No other components.
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***].

Table 11 Auditable Events

Component	Auditable Events
TrustNet Manager	Communication Operations and Failures with the CEP
	Web interface connections
	Administrative activity (configuration, etc.)
	TrustNet Manager output when TrustNet Manager starts/stops
	Activities regarding updates, access activity
CEP	System startup and shutdown, includes reboots and power cycles
	Successful and unsuccessful login attempts, log out activity, account disabled
	Additions, modifications, and deletions of Certes Enforcement Point user attributes
	Any administrative functions that result in a change to the appliance configuration and data traffic policy deployments
	Certificate addition or removal messages
	Appliance software upgrade status, formatted file system
	Failure state entered

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 , and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [*no other audit-relevant information*].

Dependencies: FPT_STM.1 Reliable time stamps

FAU_SAR.1 Audit review
Hierarchical to: No other components.
FAU_SAR.1.1

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

Dependencies: FAU_GEN.1 Audit data generation

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
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 below*] and specified cryptographic key sizes [*cryptographic key sizes – see Table 12 below*] that meet the following: [*list of standards – see Table 12 below*].

Table 12 Cryptographic Key Genetration Standards for the Certes Enforcement Points

Key Generation Type	Key Size	Standards (Certificate #)
Rivest, Shamir and Adleman (RSA)	1024, 1536, 2048, 3072, 4096	FIPS 186-3 (Certificate # 998)
DSA (Digital Signature Algorithm)	1024	FIPS 186-2 (Certificate # 615)
Pseudo Random Number Generator	256	ANSI X9.31 (Certificate # 1017)

Dependencies: FCS_COP.1 Cryptographic operation
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
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*].

Dependencies: FCS_CKM.1 Cryptographic key generation

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
FCS_COP.1.1

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

Table 13 Cryptographic Operations of the Certes Enforcement Point

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
Digital Signature verification	RSA	1024, 1536, 2048, 3072, 4096	FIPS 186-3 (Certificate #998)
	DSA	1024	FIPS 186-2 (Certificate

Cryptographic Operations	Cryptographic Algorithm	Key Sizes (bits)	Standards (Certificate #)
			#615)
Symmetric encryption and decryption	AES (CBC[12] mode)	128, 192, 256	FIPS 197 (Certificate #465, #762, #779, #1842, and #1932)
	Triple-DES (CBC mode)	168	FIPS 46-3 (Certificate #482, #667, #673, #1195, and #1258)
Message Authentication	HMAC[13] - SHA -1[14] (MAC[15] size 160)	160	FIPS 198 (Certificate #416, #417, #426, #1141, and #1166)
Message Digest	SHA	160, 256, 384, 512	FIPS 180-3 (Certificate #1697)

Dependencies: **FCS_CKM.1 Cryptographic key generation**
FCS_CKM.4 Cryptographic key destruction

Application note: RSA key-wrapping and unwrapping is used for key establishment only.

[12] CBC - Cipher Block Chaining
[13] HMAC - Hash Message Authentication Code
[14] SHA-1 - Secure Hash Algorithm 1
[15] MAC – Message Authentication Code

6.2.3 Class FDP: User Data Protection

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1
The TSF shall enforce the [*Information Flow Control SFP*] on
[
Subjects: External IT entities[16] *that send or receive information through the TOE*
Information: Ethernet Frames, or IP packets
Operations: Encrypt/decrypt, clear or drop
]
Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.
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*].

---

[16] 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.).

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

FDP_UCT.1 Basic data exchange confidentiality

Hierarchical to: **No other components.**

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.

Dependencies: **FTP_ITC.1 Inter-TSF trusted channel**
FDP_IFC.1 Subset information flow control

FDP_UIT.1 Data exchange integrity

Hierarchical to: **No other components.**

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 and insertion] has occurred.

Dependencies: **FDP_IFC.1 Subset information flow control**
FTP_ITC.1 Inter-TSF trusted channel

6.2.4 Class FIA: Identification and Authentication

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components.
FIA_SOS.1.1

The TSF shall provide a mechanism to verify that secrets meet *[a defined quality metric – see Table 14 below]*.

Table 14 Password Conventions

Component	Parameters	Conventions
TrustNet Manager Users	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
CEP	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

Dependencies: No dependencies

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1 Timing of authentication
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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UID.2 User identification before any action
Hierarchical to: FIA_UID.1 Timing of identification

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.

Dependencies: No dependencies

6.2.5 Class FMT: Security Management

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

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, Policy Deployer*].

Dependencies: FDP_IFC.1 Subset information flow control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

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, Policy Deployer*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

The TSF shall restrict the ability to [*operations – **see** Table 15 and* Table 16 ***below***] the [*list of TSF data – see Table 15 and Table 16 below*] to [*the authorized identified roles – see Table 15 and Table 16 below*].

Table 15 Management of TSF data for TrustNet Manager

Operation	TSF Data	Platform Admin	Admin	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					

Operation	TSF Data	Platform Admin	Admin	User	Appliance Admin	Appliance Operator	Policy Creator	Policy Deployer
Modify	User's assigned role	X	X					
View	Audit logs and performance statistics	X	X	X	X	X	X	X
Purge	Audit logs	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 16 Management of TSF data for CEP

Operation	TSF Data	Admin	Ops
Modify	Users and Passwords	X	
Create, Delete	Users	X	
Modify	Usernames and passwords	X	
Change	Own password	X	X
Modify	User's assigned role	X	
View	Audit logs and performance statistics	X	X
Configure	Policies	X	

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [*management of security attributes management of TSF data – see Table 15 and Table 16]*.

Dependencies: No Dependencies

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1

The TSF shall maintain the roles [*the authorized identified roles – **see** Table 17 **below***].

Table 17 User Roles

Component	Roles
TrustNet Manager	Platform Administrator
	Administrator
	Appliance Administrator
	Appliance Operator
	Policy Creator
	Policy Deployer
	User
CEP	Administrator
	Ops

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

Dependencies: FIA_UID.1 Timing of identification

6.2.6 Class FPT: Protection of the TSF

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
FPT_STM.1.1
The TSF shall be able to provide reliable time stamps **for CEP**.
Dependencies: No dependencies

6.2.7 Class FTA: TOE Access

FTA_SSL.3 TSF-initiated termination
Hierarchical to: No other components.
FTA_SSL.3.1
The TSF shall terminate an interactive session after a [*configurable inactivity period*].
Dependencies: No dependencies

6.2.8 Class FTP: Trusted Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.

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, another trusted IT product[17]] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*management sessions and communication sessions*].

Dependencies: No dependencies

[17] For this SFR, trusted IT product could refer to a user workstation sending encrypted traffic through the CEP or from another CEP, or a management workstation used by an administrator to configure the TOE.

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 18 summarizes the requirements.

Table 18 Assurance Requirements

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

7 TOE Summary 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 Functions

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 19 Mapping of TOE Security Functions to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	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_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 the TSF	FPT_STM.1	Reliable Time Stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted Channels	FTP_ITC.1	Inter-TSF trusted channel

7.1.1 Security Audit

The TNM v3.4 with CEP 10, CEP 100, CEP 1000, and CEP 10G VSEs Running CEP v2.1.1 Firmware audit function generates audit records for all system events related to audit, authentication, administration activities, and communication with external IT devices (users attempting to establish a connection with the CEP). These records contain the following information:

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

Audit records are generated by the various TOE components where auditable events occur. The auditable events for each component are specified in Table 11. The TOE provides reliable time stamps for the CEP appliance, and the TOE environment provides time stamps TrustNet Manager component of the TOE. The TOE requires that the clocks on all the TOE components be synchronized so that the TOE can accurately record the time each event occurred. For this purpose all the TOE components are synchronized with an NTP server.

CEP log files are stored in the CEP file system. The logs can be retrieved and viewed for any CEP appliances through TrustNet Manager. Audit records are displayed in a human-readable format. The log files of TrustNet Manager are accessible through the web interface.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_SAR.1,

7.1.2 Cryptographic Support

The TOE provides for secure communication between two CEP appliances and between a CEP appliance and a trusted remote IT product (management workstation). The cryptographic module of the CEP is capable of:

- performing symmetric encryption and decryption with Triple-DES; AES-128, AES-192, and AES-256
- message authentication with HMAC-SHA-1 and pre-shared secrets
- key generation with ANSI X9.31 PRNG to produce AES 256 bit keys or Triple-DES 192 bit keys

The Cryptographic Support function provides encryption and decryption of all data transmitted between the CEP appliances, or a CEP appliance and a trusted external IT entity (users who have successfully authenticated with the CEP).

1. CEP to CEP encryption – The CEP has two data ports: the local port and the remote port which interface with other network equipment. Unencrypted traffic that originates from a trusted, local network is received on the local port of the origination CEP. This CEP then encrypts the received traffic based on the configured policies and encryption parameters, and sends it out through the remote port to another CEP via an untrusted network, such as the Internet. At the receiving CEP, the process is reversed; encrypted traffic is received on the CEP remote port and decrypted using the information from the same policy used during the encryption process. Then the decrypted traffic is sent from the local port to the final destination. All encryption for CEP to CEP communication uses cryptographic algorithms provided by a FIPS 140-2 validated cryptographic module.

2. Management workstation to CEP encryption – Management traffic may enter the CEP through the CLI and is secured using SSH. Encryption between the management workstation and the CEP appliance is provided by the FIPS 140-2 validated cryptographic module.

The CEP appliance's FIPS 140-2 validated cryptographic module is capable of generating keys for Triple-DES (192 bits), AES-128, AES-192, and AES-256 using the ANSI X9.31 PRNG. The Triple-DES and AES ciphers operate in CBC mode.

The FIPS 140-2 validated cryptographic module also uses RSA (key sizes 1024, 1536, 2048, 3072, 4096 bits) for key establishment and HMAC-SHA-1 (160 bits) for message authentication.

The TOE destroys cryptographic keys in accordance with FIPS 140-2 zeroization requirements. TOE session keys are destroyed after the SA lifetime has expired.

TOE Security Functional Requirements Satisfied: FCS_CKM.1, 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: 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 Encapsulating Security Payload (ESP) as the IPSec security protocol which provides confidentiality, integrity, and data origin authentication. The TOE provides confidentiality services by implementing the AES and Triple-DES ciphers in CBC mode. The TOE generates cryptographic keys required for encryption in accordance with the AES and Triple-DES algorithms. Keys are destroyed after the SA has expired. The TOE provides integrity services by implementing SHA-1. The TOE provides data origin authentication services for the IP packet or Ethernet frame by implementing HMAC-SHA-1. For each packet or frame, this creates a cryptographic checksum ensuring that only the external IT entities (users sending traffic through the CEP) have 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.

7.1.4 Identification and Authentication

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

The TOE requires the operator to enter a correct username and password before allowing any action to take place. Administrator and User authentication is enabled by default for TrustNet Manager. Administrator and Ops authentication is enabled by default for CEP. Role-based authorization is enabled by default for

TrustNet Manager. 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 TrustNet Manager 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 password requirements for different TOE components are as specified in Table 14.

TOE Security Functional Requirements Satisfied: FIA_SOS.1, FIA_UAU.2, 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 15 and Table 16 above.

The TOE provides the authorized user the capability to configure the TOE and its security policies to secure the data and management paths. TrustNet Manager provides seven roles for managing its security functions: Platform Administrator, Administrator, Appliance Administrator, Appliance Operator, Policy Creator, Policy Deployer, User. The TSF maintains a list of permissions for all seven roles. When a user logs in and authenticates through the management interfaces, the TSF shall be able to associate users with one or more of the above roles. Refer to Table 15 and Table 16 for the privileges associated with the TrustNet Manager roles.

The CEP Administrator has privileges to manage the appliance users and CLI. The Ops is only able to log in to the CLI.

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 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 TrustNet Manager is installed on is not included in the TOE boundary and therefore the TOE Environment provides the reliable timestamps for TrustNet Manager. All the TOE component's times are synchronized with the NTP server. By the value of the timestamps the order of the audit records are determined. 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_STM.1.

7.1.7 TOE Access

The TOE will terminate an administrator CLI or End User TrustNet Manager 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 or End User is logged out.

TOE Security Functional Requirements Satisfied: FTA_SSL.3

7.1.8 Trusted Channels

The trusted channels function guarantees a secure channel that the TOE (Certes Enforcement Point) can use to communicate with a trusted remote IT product (management workstation via SSH or another Certes Enforcement Point). Likewise, the external entity can initiate communications to the TOE via this secure channel. Encryption-based protection is provided for the communication channels as identified in Table 13.

TOE Security Functional Requirements Satisfied: FTP_ITC.1

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Parts 2 and 3 of the Common Criteria Standard for Information Technology Security Evaluations, version 3.1 Revision 2. There are no extended SFRs contained within this ST.

There are no protection profile claims for this Security Target.

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 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 20 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.NO_AUDIT An attacker may perform security-relevant operations on the TOE without being held accountable for it.	O.AUDIT The TOE must record events of security relevance with accurate dates and timestamps. The TOE must provide the authorized administrators with the ability to review the audit records.	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 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.
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.KEYMAN The TOE must provide the means for secure management of cryptographic keys. This includes 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.ENCRYPT The TOE must provide the means of protecting the confidentiality of	O.ENCRYPT counters this threat by ensuring that the information traveling over a public network

Threats	Objectives	Rationale
	information transferred across a public network between two protected networks using cryptography that conforms to standards specified in FIPS PUB 140-2.	can not be intercepted by an un-authorized person. The confidentiality is assured by encryption operation.
	O.SECURE_COMM The TOE shall securely transfer data between a CEP device and management workstation and a CEP device and another CEP device.	O.SECURE_COMM counters this threat by ensuring that any management data traveling between two CEPs or a CEP and a management workstation 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 management workstation and a CEP device and another CEP device.	O.SECURE_COMM counters this threat by ensuring that any management data traveling between the CEP and a management workstation is not modified.
T.UNATH An unauthorized person may gain access to the TOE and compromise its security functions by changing its configuration.	O.AUDIT The TOE must record events of security relevance with accurate dates and timestamps. The TOE must provide the authorized administrators with the ability to review the audit records.	O.AUDIT counters this threat by ensuring that unauthorized attempts to access the TOE are recorded.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its security functions, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN counters this threat by ensuring that only authorized users have access to TOE management functions.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE	O.AUTHENTICATE counters this threat by ensuring that users are identified and authenticated prior to gaining access to TOE security

Threats	Objectives	Rationale
	administrative functions and data.	data.
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 management workstation and a CEP device and another CEP device.	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.

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 21 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	OE.TIMESTAMP NTP servers providing time	OE.TIMESTAMP upholds this assumption by ensuring that TOE

Assumptions	Objectives	Rationale
TrustNet Manager with the necessary reliable timestamps.	information to the TOE shall be on the local network and inaccessible to non-administrators.	environment providing time stamps are on the local network and in-accessible to non-administrators.
A.LOCATE The connection between the CEP and TNM, management workstation which is connected to TNM, and TOE Environmental components (the NTP, SNMP, and syslog servers) are all located within a controlled access facility behind on 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 Local Area Network that the CEP and TNM, and Management workstation used for TNM, 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 Local Area Network are protected from outside attacks.
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.

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 22 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance with accurate dates and timestamps. The TOE must provide the authorized administrators with the ability to review the audit records.	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_SAR.1 Audit review	This requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FPT_STM.1 Reliable Time Stamps	This requirement meets the objective by ensuring that the TOE can provide reliable time stamps. The time stamps allow the TOE to place events in the order that they occurred.
O.ADMIN The TOE must include a set of functions that allow efficient management of its security functions, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FAU_SAR.1 Audit review	This requirement meets the objective by ensuring that the TOE makes the audited records available for authorized users.
	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.

Objective	Requirements Addressing the Objective	Rationale
	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	This requirement supports the objective. The informational flow control policy is permissive by default.
	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.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and 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_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.

Objective	Requirements Addressing the Objective	Rationale
	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.
O.KEYMAN The TOE must provide the means for secure management of cryptographic keys. This includes 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.4 Cryptographic key destruction	This requirement meets the objective by ensuring that the cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	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.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.4 Cryptographic key destruction	This requirement meets the objective by ensuring that the cryptographic keys are destroyed according to FIPS 140-2 zeroization requirements.
	FCS_COP.1	This requirement meets the

Objective	Requirements Addressing the Objective	Rationale
	Cryptographic operation	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	FCS_COP.1	This requirement meets the

Objective	Requirements Addressing the Objective	Rationale
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.	Cryptographic operation	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.SECURE_COMM The TOE shall securely transfer data between a CEP device and management workstation and a CEP device and another CEP device.	FTP_ITC.1 Inter-TSF trusted channel	This requirement meets the objective by ensuring that any management data transfer between TOE components happens over a trusted channel.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was selected 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.
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

This ST does satisfy all the requirement dependencies of the Common Criteria. Table 23 lists each requirement to which the TOE claims conformance with a dependency and indicates whether the dependent requirement was included. As the table indicates, all dependencies have been met.

Table 23 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	
FDP_UCT.1	FTP_ITC.1	✓	
	FDP_IFC.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_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_STM.1	No dependencies		
FTA_SSL.3	No dependencies		
FTP_ITC.1	No dependencies		

9 Acronyms

This section describes the acronyms.

Table 24 Acronyms

Acronym	Definition
ANSI	American National Standards Institute
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CEP	Certes Enforcement Point
CLI	Command Line Interface
EAL	Evaluation Assurance Level
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
HSM	Hardware Security Module
ID	Identifier
IP	Internet Protocol
IPSec	IP Security Protocol
IT	Information Technology
MAC	Message Authentication Code
Mbps	Megabits per second
NTP	Network Time Protocol
OS	Operating System
PMTU	Path Maximum Transmission Unit
PP	Protection Profile
RNG	Random Number Generator
SAD	Security Association Database
SAR	Security Assurance Requirement

Acronym	Definition
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VLAN	Virtual Local Area Network
VM	Virtual Machine
XML-RPC	Extensible Markup Language Remote Procedure Call

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway, Suite 220
Fairfax, VA 22033
United States of America

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