Forcepoint On-Premise Security 8.5

Security Target

Version 1.0
May 20, 2019

Prepared for:

Forcepoint, LLC
10900 Stonelake Blvd, 3rd Floor
Austin, TX 78759

Prepared by:

leidos

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE comprises the Forcepoint On-Premise Security 8.5 solution.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Rationale (Section 7).

1.1 Security Target, TOE and CC Identification

ST Title – Forcepoint On-Premise Security 8.5 Security Target

ST Version – Version 1.0

ST Date – April 24, 2019

TOE Identification –

- Forcepoint On-Premise Security v8.5 running on V10000 G4 appliance with the following specifications:
    - Dell Platform Name: R430
    - CPU: Intel E5-2620 v3 X2
    - Memory:
    - Ports:
        - 4 x onboard NICs
        - 1 x 2 port addon NIC
        - VGA display connector
        - Serial port connector
        - Power supply connector
    - On-board NIC: Broadcom 4P 5720
    - Addon NIC: Broadcom 2P 5720 or Intel 10G 2P X520 or Intel 10G 2P X520 + Intel 10G 2P X710
    - Hard drive: 300GB SAS X4
    - RAID controller: PERC H730 Mini

TOE Developer – Forcepoint

Evaluation Sponsor – Forcepoint

CC Identification – *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017*

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017
  - Part 3 Conformant

The ST and the TOE it describes are conformant to the following package:

- EAL2 Augmented (ALC_FLR.2).

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by appending the SFR with parentheses that contain a letter that is unique for each iteration, e.g. (a), (b), (c) and a descriptive string for the SFR's purpose, e.g. Server.
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Abbreviations and Acronyms

AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher-Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
DEK	Data Encryption Key
DLP	Data Loss Prevention
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EE	Encryption Engine
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HMAC	Hashed Message Authentication Code

IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
KMD	Key Management Description
RBG	Random Bit Generator
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SAR	Security Assurance Requirement
SED	Self Encrypting Drive
SHA	Secure Hash Algorithm
SFP	Security Functional Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
SPI	Serial Peripheral Interface
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
XOR	Exclusive or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2. TOE Description

The TOE consists of version 8.5 of Forcepoint’s On-Premise Security running on Forcepoint V-Series Security Appliances. The V10000 G4 appliance model is included as part of the TOE.

The TOE is a unified solution providing data protection. On-Premise Security 8.5 provides an email gateway and web scanning services, as well as data loss prevention capabilities.

2.1 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 describing the product, and defining the specific evaluated deployment.

On-Premise Security 8.5 provides a data theft prevention solution to secure an organization’s data on and off the organization network. The protection provided by On-Premise Security is delivered by three main components, namely Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security, and the supporting components Forcepoint DLP Endpoint. These components work together to prevent security breaches, productivity loss, and legal issues that might arise due to inappropriate or careless browsing, email messaging and network usage habits. The components are managed using the Forcepoint Security Manager (FSM).

The On-Premise Security solution is highly scalable according to customer strategy to address data theft and data loss. The Forcepoint Web Security, Forcepoint DLP and Forcepoint Email Security can be deployed as individually to address specific customer needs for data theft and loss through specific organization network activities. These solutions can be physical on-premise installations, hybrid deployments or cloud-based deployments. The evaluated deployment of On-Premise Security consists of Forcepoint Web Security and Forcepoint Email Security components installed on Forcepoint V-Series Security Appliances with the other On-Premise Security components installed on customer-supplied on-premise platforms.

2.2 TOE Architecture

2.2.1 Physical Boundaries

The TOE is the On-Premise Security 8.5 solution, including the V-Series appliance on which the Forcepoint Web Security and Forcepoint Email Security components are installed.

The other On-Premise Security 8.5 components with the exception of DLP endpoints run on Microsoft Windows Servers and Linux-based soft-appliances. In the evaluated configuration they must be running on Windows Server 2012 or highter. The V-Series appliance hardware is a Dell PowerEdge server with an Intel Xeon processors running a customized version of the CentOS 7 operating system.

These comprise the following components:

- Forcepoint Security Manager 8.5
- Forcepoint Security Appliance Manager 2.0
- Forcepoint Web Security Appliance 8.5
- Forcepoint Email Security Appliance 8.5
- Forcepoint DLP Server 8.5
- Forcepoint DLP Analytics Engine 8.5
- Forcepoint DLP Endpoint 8.5 (Windows)
- Forcepoint DLP Endpoint 8.5 (MacOS).

In addition to physical platforms, the Analytics Engine, Web Security Appliance and Email Security Appliances can be deployed on virtualized hardware. The TOE supports VMware ESX v6.0.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by the TOE

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- TOE Access

2.2.2.1 Security Audit

The TOE generates audit logs of Forcepoint Security Manager activity; recording administrator login attempts, logoffs, policy changes, and configuration changes in the Audit Logs for each component. Only Super Administrators and System Administrators can review the audit logs.

The TOE provides reliable timestamps to accurately record the sequence of events within the audit records.

2.2.2.2 Cryptographic Support

All cryptographic functionality is performed by one of the TOE's FIPS certified cryptographic modules. The Forcepoint C Cryptographic Module (CMVP Certificate #2875) is used to protect communications between TOE components, while the Forcepoint Java Cryptographic Module (CMVP Certificate #3113) is used to protect communications between servers and remote management workstations.

2.2.2.3 User Data Protection

The TOE enforces web, data and email filters and policies on user traffic (inbound and/or outbound) to prevents internal entities from accessing potentially harmful or inappropriate content on external data, prevent loss of organization data and prevent infected email from entering the network. The TOE also supports data classification through the use of the Boldon James tagging system.

2.2.2.4 Identification and Authentication

The TOE enforces identification and authentication for administrators before they can access any management functionality via the CLI or GUI.

The TOE also prevents administrators from accessing FSM and FSAM content before providing and authenticating a valid identity. The TOE maintains a list of security attributes (such as login credentials) for administrators. Authentication can be done either with a username and password or X.509 certificates.

Depending on the web policy applied, unprivileged users are able to browse the internet anonymously.

Email users have to identify and authenticate themselves before the TOE will permit access to their Personal Email Management UI to manage quarantined email messages.

2.2.2.5 Security Management

The TOE provides robust management interfaces that authorized administrators can use to manage the TOE and configure policies to control access to content. By default proxy filtering is enabled, but all traffic is allowed; therefore, the TOE has a permissive default posture.

The TOE defines two categories of administrator — Security Administrator and Delegated Administrator.

System Administrator roles manage system-wide operations, such as setting domains, editing user profiles and permissions, and setting up routes and preferences across all Web, Email, and Data components. See the table in section 5.2.5.9 for further details on Security Administrator roles.

Policy Administrators have custom permission sets defined by associating the Delegated Administrator with one or more roles (set of access privileges) across a single Email, Web and DLP component. For example, a Policy

Administrator can be granted “Super Administrator” role in the Web component to manage user profiles, permissions, profiles and settings, similar to a System Administrator role, but limited to only the Web component.

There are eight other permission sets that can be applied to Policy Administrator to manage one or more of the components within FSM.

2.2.2.6 Protection of the TSF

Communications between the DLP Server and DLP endpoints are protected by TLS to protect them from disclosure and modification. This protects the policies that are to be implemented on client devices as well as actions taken by clients as a results of policies being applied. Logical protection of these communications is necessary since DLP endpoints are not co-located with the remainder of the TOE and as such do no benefits from the physical protection of a secure facility.

2.2.2.7 Resource Utilization

The TOE enforces maximum limits on usage and availability of controlled traffic. The TOE is capable of limiting access to specific sites, imposing time constraints on use and capping individual user bandwidth use.

2.2.2.8 TOE Access

The TOE can assign a limit on the number of concurrent sessions that administrative users are allowed to have with FSM. If this limit is reached, the TOE prevents any new sessions from being created.

A FSM console session ends 22 minutes after the last action taken in the user interface (clicking from page to page, entering information, caching changes, or saving changes). A warning message is displayed 5 minutes before session end.

2.3 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific guides reference the security-related guidance material for all devices in the evaluated configuration:

- *Preparative Procedures*
- *User Guide*
- *Administrative Guidance*
- *Other*

If documentation is provided online please provide URLs:

3. Security Problem Definition

This section defines the security problem to be addressed by the TOE, in terms of threats to be countered by the TOE or its operational environment, assumptions about the intended operational environment of the TOE, and Organizational Security Policies (OSPs) that apply to the TOE.

3.1 Assumptions

This section contains assumptions regarding the operational environment and the intended usage of the TOE.

A.INSTALL On-Premise Security has been installed and configured according to the appropriate installation guides.

A.NETWORK All policy-controlled traffic between the internal and external networks traverses On-Premise Security.

A.LOCATE It is assumed that the On-Premise Security appliance and associated servers are located within the same controlled-access facility and exclude unauthorized access to the internal physical network.

A.NOEVIL It is assumed that administrators who manage On-Premise Security are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance. Similarly is it assumed that users of the DLP endpoint component are not negligent or willfully hostile.

A.MANAGE There are one or more competent individuals assigned to manage On-Premise Security and the security of the information it contains.

3.2 Threats

T.EXTERNAL_CONTENT **Error! Reference source not found.**

T.DATA_LOSS **Error! Reference source not found.**

T.MASQUERADE A user may masquerade as another entity in order to gain unauthorized access to user data or On-Premise Security controlled resources.

T.NACCESS An unauthorized person or external IT entity may be able to view or modify On-Premise Security configuration and control data by hijacking an unattended administrator session.

T.UNAUTHORIZED_ACCESS A user may gain access to security data controlled by On-Premise Security that they are not authorized to access.

T.RESOURCE On-Premise Security users or attackers may cause network connection resources to become overused and therefore unavailable.

3.3 Organizational Security Policies

There are no Organizational Security Policies defined for this ST.

4. Security Objectives

This section identifies the security objectives for the TOE and its operational environment. The security objectives identify the responsibilities of the TOE and its environment in addressing the security problem defined in Section 3.

4.1 Security Objectives for the TOE

The following are the TOE security objectives:

O.AUTHENTICATE
The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.

O.AUDIT
The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record system configuration and traffic policy updates and allow trained administrators to review security-relevant audit events.

O.MANAGE
The TOE must provide secure management of the system configuration and the traffic policies over one or more concurrent sessions.

O.RESOURCE_CONTROL
The TOE must control access to network resources as defined by the traffic policies.

O.DATA_PROTECT
The TOE will take specified actions against transmission of identified files or data.

O.QUOTA
The TOE must be able to place quotas on network connection resources.

O.TIMESTAMP
The TOE must provide a timestamp for its own use.

O.HARMFUL_CONTENT
The TOE must disallow access to malicious content hidden within legitimate network resource requests.

O.PROTECT
The TOE must have the capability to protect configuration data from unauthorized reading or modification.

4.2 Security Objectives for the Operational Environment

The following are the security objectives for the operational environment of the TOE:

OE.NETWORK
All policy-controlled protocol traffic between the internal and external network must traverse the TOE.

OE.PROTECT
The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE server components, between FSAM and the administrator, and between TOE components and (optional) authentication server.

OE.CLIENT
The endpoint client workstations must be logically protected using best security practices, including the installation of anti-virus and anti-spyware software and configuration of PC firewall.

OE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.

OE.USER The Authorized users are trusted to not actively or negligently compromise the security of the component on which the TOE Endpoint component is installed.

OE.LOCATE The physical environment must be suitable for supporting computing devices in a physically secure setting.

Note:
All of the cryptographic functionality is implemented by the TOE and the TOE does not rely on its Operational Environment to provide any cryptographic services. Therefore OE.STRONG_ENVIRONMENT_CRYPTO is not included in the ST.

5. IT Security Requirements

The security requirements for the TOE have been drawn from Parts 2 and 3 of the Common Criteria. The security functional requirements have been selected to correspond to the actual security functions implemented by the TOE while the assurance requirements have been selected to offer a low to moderate degree of assurance that those security functions are properly realized.

5.1 Extended Component Definition

This Security Target includes Security Functional Requirements (SFRs) that are not drawn from CC Part 2. These Extended SFRs are identified by having a label '_EXT' after the requirement name for TOE SFRs. The structure of the extended SFRs is modeled after the SFRs included in CC Part 2. The structure is as follows:

A. Class – The extended SFRs included in this ST are part of the identified classes of requirements.

B. Family – The extended SFRs included in this ST are part of several SFR families including the new families defined below.

C. Component – The extended SFRs are not hierarchical to any other components, though they may have identifiers terminating on other than "1". The dependencies for the extended components are identified both in this section and in the TOE SFR Dependencies section of this ST (Section **Error! Reference source not found.**, **Error! Reference source not found.**).

5.1.1 Extended Family Definitions

5.1.1.1 FAU_GEN_EXT

Family Behavior

This family is added to the class FAU. This family defines requirements for recording the occurrence of security relevant events that take place under TSF control, and is based on the FAU_GEN family without the requirement to audit the start-up and shutdown of auditing mechanisms (which is not directly transferable to a TOE with distributed, independent components).

Management: FAU_GEN_EXT.1

There are no management activities foreseen

Audit: FAU_GEN_EXT.1

There are no auditable activities foreseen.

Security Audit Generation (FAU_GEN_EXT.1)

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamps

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

a) All auditable events for the [selection, choose one of: minimum, basic, detailed, not specified] level of audit; and
b) [assignment: other specifically defined auditable events].

FAU_GEN_EXT.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, [assignment: *other audit relevant information*].

5.1.2 Extended Requirements Rationale

FAU_GEN_EXT.1.1 is an extended functional requirement that was created to closely match the requirements of FAU_GEN.1, defined in Common Criteria Part 2, but without the requirement for auditing start-up and shutdown events for the TOE, which are not applicable to this TOE with distributed components.

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN_EXT.1: Audit data generation
	FAU_SAR.1: Audit review
	FAU_SAR.2: Restricted audit review
FCS: Cryptographic Support	FCS_CKM.1:Cryptographic key generation
	FCS_CKM.4: Cryptographic key destruction
	FCS_COP.1(a): Cryptographic operation (KeyPair Generation)
	FCS_COP.1(b): Cryptographic operation (Encryption)
	FCS_COP.1(c): Cryptographic operation (Hashing)
	FCS_COP.1(d): Cryptographic operation (Cryptographic Signature Services)
FDP: User Data Protection	FDP_ACC.1(a): Subset access control
	FDP_ACF.1(a): Security attribute based access control
	FDP_ACC.1(b): Subset access control
	FDP_ACF.1(b): Security attribute based access control
	FDP_ACC.1(c): Subset access control
	FDP_ACF.1(c): Security attribute based access control
FIA: Identification and Authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of Authentication
	FIA_UAU.2: User authentication before any action
	FIA_UID.1: Timing of identification
	FIA_UID.2: User identification before any action
FMT: Security Management	FMT_MOF.1: Management of security functions behaviour
	FMT_MSA.1(a): Management of security attributes (change)
	FMT_MSA.1(b): Management of security attributes (View)
	FMT_MSA.3(a): Static attribute initialization
	FMT_MSA.3(b): Static attribute initialization
	FMT_MSA.3(c): Static attribute initialization

Requirement Class	Requirement Component
	FMT_MTD.1: Management of TSF data
	FMT_SAE.1: Time-limited authorisation
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_STM.1: Reliable time stamps
	FPT_ITT.1: Basic internal TSF data transfer protection
FRU: Resource Utilisation	FRU_RSA.1(a): Maximum quotas
	FRU_RSA.1(b): Maximum quotas
FTA: TOE Access	FTA_MCS.2: Per user attribute limitation on multiple concurrent sessions
	FTA_SSL.3: TSF-initiated termination

TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation (FSM Audit Log) (FAU_GEN_EXT.1)

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

a) All auditable events, for the [***not specified***] level of audit; and

b) [**successful administrator logins, administrator logoffs, internet usage filter changes, web protection policy changes, email filter changes, email policy changes, data loss prevention policy changes, and appliance configuration changes**].

FAU_GEN_EXT.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, [**server affected by the change (IP address) and role affected**].

5.2.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**Super Administrator, System Administrator**] with the capability to read [**all audit data**] from the audit records.

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

5.2.1.3 Restricted Audit Review (FAU_SAR.2)

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

5.2.2 Cryptographic Support (FCS)

5.2.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**HMAC DRBG (AES), RSA**] and specified cryptographic key sizes [**128 bits (AES), 256 bits (AES), 2048 bits (RSA)**] that meet the following: [**SP800-90A, X9.31**].

5.2.2.2 Cryptographic Key Destruction (FCS_CKM.4)

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**key zeroization**] that meets the following: [**FIPS 140-2**].

5.2.2.3 Cryptographic Operation (KeyPair Generation) (FCS_COP.1(a))

FCS_COP.1.1(a) The TSF shall perform [**keypair generation**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bits**] that meets the following: [

- **X9.31].**

5.2.2.4 Cryptographic Operation (Encryption) (FCS_COP.1(b))

FCS_COP.1.1(b) The TSF shall perform [**Encryption**] in accordance with a specified cryptographic algorithm [**3DES, AES(CBC), AES(GCM)**] and cryptographic key sizes [**128, 168, 256 bits**] that meets the following: [

- **3DES: ISO 18033-3**
- **AES: ISO 18033-3 CBC mode: ISO 10116 GCM mode: ISO 8802-1**]

5.2.2.5 Cryptographic Operation (Hashing) (FCS_COP.1(c))

FCS_COP.1.1(c) The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256, SHA-384**] and ~~cryptographic key~~ **message digest** sizes [**160, 256, 384**] that meets the following: [

- **ISO 10118-3**]

5.2.2.6 Cryptographic Operation (Cryptographic Signature Services) (FCS_COP.1(d))

FCS_COP.1.1(d) The TSF shall perform [**cryptographic signature services**] in accordance with a specified cryptographic algorithm [**RSA Digital Signature Algorithm (rDSA)**] and cryptographic key sizes [**2048 bits**] that meets the following: [

- **X9.31].**

5.2.3 User Data Protection (FDP)

5.2.3.1 Subset Access Control (FDP_ACC.1(a))

FDP_ACC.1.1(a) The TSF shall enforce the [**internet access policy**] on [

1. **Subjects: users**
2. **Objects: external IT entities hosting content**
3. **Operations: Retrieving hosted content].**

5.2.3.2 Security Attribute Based Access Control (Web) (FDP_ACF.1(a))

FDP_ACF.1.1(a) The TSF shall enforce the [**Internet Access Policy**] to objects based on the following:

[**Subject Attributes:**

1. **User name**
2. **User group**
3. **IP address**
4. **Quota for Access**

Object Attributes:

1. **Assigned category**
2. **IP address**
3. **URL**
4. **Protocol**
5. **Keywords**
6. **Web Objects**

]

FDP_ACF.1.2(a) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. **If a bandwidth usage quota is defined for the category or protocol, evaluate the current bandwidth:**
   a. **If the bandwidth currently in use is below the defined threshold for the category or protocol, allow access to the content.**
   b. **If the bandwidth currently in use is above or at the defined threshold for the category or protocol, deny access to the content.**
2. **If a "block" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "block page".**
3. **If a "permit" rule is defined for the category or protocol group, allow access to the content.**
4. **If a "confirm" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "confirmation page" until the user confirms that the access is for business-related purposes.**
5. **If a "quota" rule is defined for the category or protocol group, deny access to the content and redirect the user to the "quota confirmation page". If the user agrees to continue to the content, begin the quota timer for the user.**
6. **If no rule is defined for the content, allow access to the requested content**

].

FDP_ACF.1.3(a) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4(a) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[if a "quota" rule is defined and a user has no more browsing quota, the TOE denies access to the user and shows the "block" page].**

5.2.3.3 Subset Access Control (FDP_ACC.1(b))

FDP_ACC.1.1(b) The TSF shall enforce the [**Data Loss Prevention Policy**] on [

1. **Subjects: users**
2. **Objects: filesystem files, email messages, database entries**
3. **Operations: file access, email transmission, database update**].

5.2.3.4 Security Attribute Based Access Control (Data) (FDP_ACF.1(b))

FDP_ACF.1.1(b) The TSF shall enforce the [**Data Loss Prevention Policy**] to objects based on the following:

[

Subject Attributes:

1. **User name**
2. **User group**
3. **Domain**

Object Attributes

1. **Resource type**
2. **Content Classifier**

].

FDP_ACF.1.2(b) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. **If the accumulated number of matched rules for subject and object attributes is below the threshold (Drip DLP)**
2. **If the number of matched rules for a single transaction matching subject and object attributes is below the threshold**

].

FDP_ACF.1.3(b) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[no additional rules]**.

FDP_ACF.1.4(b) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[no additional rules]**.

5.2.3.5 Subset Access Control (FDP_ACC.1(c))

FDP_ACC.1.1(c) The TSF shall enforce the [**Email Policy**] on [

1. **Subjects: users**
2. **Objects: email messages, email attachments**
3. **Operations: receiving email, sending email**].

5.2.3.6 Security Attribute Based Access Control (Email) (FDP_ACF.1(c))

FDP_ACF.1.1(c) The TSF shall enforce the [**Email Policy**] to objects based on the following:

[

Subject Attributes:

1. **Email Address**
2. **Group**
3. **IP Address**
4. **Sender**

Object Attributes

1. **Direction of email message**
2. **Email message macro content**

].

FDP_ACF.1.2(c) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[

1. **If message subject and object attributes match a rule with a "Deliver message" action, or**
2. **If message subject and object attributes match a "Resume processing" action as the final filter in the sequence of filters applied to the message**

].

FDP_ACF.1.3(c) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**message matches Always Permit List**].

FDP_ACF.1.4(c) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[message matches Always Block List, or message matches a rule a "Drop message" action].**

5.2.4 Identification and Authentication (FIA)

5.2.4.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual ~~users~~ **administrators: [user name, role, password].**

5.2.4.2 Timing of Authentication (Administrator) (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow **[access to the installation CLI]** on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is authenticated.

FIA_UAU.1.2 The TSF shall require each ~~user~~ **administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

5.2.4.3 User Authentication Before Any Action (Web/Email User) (FIA_UAU.2)

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

5.2.4.4 Timing of Identification (Administrator) (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow [**access to the installation CLI**] on behalf of the ~~user~~ **administrator** to be performed before the ~~user~~ **administrator** is identified.

FIA_UID.1.2 The TSF shall require each ~~user~~ **administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that ~~user~~ **administrator**.

5.2.4.5 User Identification Before Any Action (Web/Email User) (FIA_UID.2)

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.

5.2.5 Security Management (FMT)

5.2.5.1 Management of Security Functions Behavior (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable, modify the behaviour of***] the functions [**Forcepoint Web Security component, Forcepoint Email Security component, Forcepoint DLP component**] to [**Super Administrators, System Administrators and Policy Administrators**].

5.2.5.2 Management of Security Attributes (Change) (FMT_MSA.1(a))

FMT_MSA.1.1(a) The TSF shall enforce the [**Internet Access Policy, Data Loss Policy and Email Policy**] to restrict the ability to [***change_default, query, modify, delete, [create]***] the security attributes [**internet usage filters, web protection policies, email filters, email policies, data loss prevention policies, and appliance configuration**] to [**Super Administrators, System Administrator and Policy Administrator**].

5.2.5.3 Management of Security Attributes (View) (FMT_MSA.1(b))

FMT_MSA.1.1(b) The TSF shall enforce the [**Internet Access Policy, Data Loss Policy and Email Policy**] to restrict the ability to [***query***] the security attributes [**internet usage filters, web protection policies, email filters, email policies, data loss prevention policies, and appliance configuration**] to [**Super Administrators, System Administrator Policy Administrator and Auditor**].

5.2.5.4 Static Attribute Initialization (Web) (FMT_MSA.3(a))

FMT_MSA.3.1(a) The TSF shall enforce the **[Internet Access Policy]** to provide **[*permissive*]** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a) The TSF shall allow the [**Super Administrators and Policy Administrators**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.5 Static Attribute Initialization (Data) (FMT_MSA.3(b))

FMT_MSA.3.1(b) The TSF shall enforce the [**Data Loss Prevention Policy**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b) The TSF shall allow the [**Super Administrators and Policy Administrators**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.6 Static Attribute Initialization (Email) (FMT_MSA.3(c))

FMT_MSA.3.1(c) The TSF shall enforce the [**Email Policy**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(c) The TSF shall allow the [**Super Administrators and Policy Administrators**] to specify alternative initial values to override the default values when an object or information is created.

5.2.5.7 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [***query***, ***[search, sort, and select]***] the [**audit data**] to [**Super Administrators**].

5.2.5.8 Time-Limited Authorisation (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [**the administrator management session time**] to [**Super Administrators**].

FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [**terminate the administrative session**] after the expiration time for the indicated security attribute has passed.

5.2.5.9 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[management of security functions behavior, management of security attributes, and management of TSF data in accordance with the table below].**

Role	Description	Security Manager		
Global Security Administrator	Administrators with this permission set have full access across FSAM; they can add and remove administrators and edit the profiles and permissions of all other administrators.	✓		
Conditional Super Administrator	Administrators with this permission set have access to all general settings within FSAM and can add domains and set up routes and preferences. Permissions are identical to a Global Security Administrator, except they cannot manage other administrators	✓		
Delegated Administrator Role	Description	Email	Web	Data
Super Administrator	Administrators with this role have full access; they can add and remove administrators and edit the profiles and permissions of all other administrators.	✓	✓	✓
Auditor	Administrators with this role can view all configuration settings but not change them.	✓	✓	✓
Reporting Administrator	Administrators with this role can edit, run, and schedule reports only.	✓	✓	
System Administrator[1]	Administrators with this role have access to all general settings and can add domains and set up routes and preferences. Permissions are identical to a Super Administrator, except they cannot manage other administrators	✓	✓	✓
Policy Administrator	Administrators with this role can create and manage policies only for the specific users or groups managed by this role. Permissions include reporting and quarantine management for these users and groups	✓	✓	✓
Quarantine Administrator	Administrators with this role can manage specific queues, troubleshoot from logs, and release messages to users from assigned queues.	✓		
Incident Administrator	Administrator with this role can access reports, incident details, and workflow. Manages incident handling.			✓
Group Reporting Administrator	Administrators with this role can edit, run, and schedule reports only for users in specified groups.	✓		
Default	This is the default role for a new administrator. Administrators only assigned to this role can access only reports and the Today page.	✓	✓	✓
Real Time Monitor	Administrators with this role can monitor Internet traffic in real time.		✓	

On-Premise Security Delegated Administrator and FSM Administrator Roles

[1] This role is labelled “Security Administrator” in the Email delegated roles and “Conditional Super Administrator” in the Web delegated roles.

5.2.5.10 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **[**

On-Premise Security Administrator roles: Global Security Administrator, Conditional Super Administrator;

Delegated Administrator roles: Super Administrator, Auditor, Reporting Administrator, System Administrator, Policy Administrator, Quarantine Administrator, Incident Administrator, Group Reporting Administrator, Real Time Monitor Default].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Basic Internal TSF Data Transfer Protection (FPT_ITT.1)

FPT_ITT.1.1 The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.

5.2.6.2 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

5.2.7 Resource Utilisation (FRU)

5.2.7.1 Maximum Quotas (FRU_RSA.1(a))

FRU_RSA.1.1(a) The TSF shall enforce maximum quotas of the following resources: [**access to restricted approved categories**] that [***individual user***] can use [***over a specified period of time***].

5.2.7.2 Maximum Quotas (FRU_RSA.1(b))

FRU_RSA.1.1(b) The TSF shall enforce maximum quotas of the following resources [**bandwidth**] that [***defined group of users***] can use [***simultaneously***].

5.2.8 TOE Access (FTA)

5.2.8.1 Per User Attribute Limitation on Multiple Concurrent Sessions (FTA_MCS.2)

FTA_MCS.2.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user according to the rules [**if a user exceeds the bandwidth quota for a protocol category defined by policy, any new concurrent sessions within that category will be blocked**].

FTA_MCS.2.2 The TSF shall enforce, by default, a limit of **[unlimited]** sessions per user.

5.2.8.2 TSF-Initiated Termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[an administrator defined period of inactivity].**

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Requirement Class	Requirement Component
ADV: Development	ADV_ARC.1: Security architecture description
	ADV_FSP.2: Security-enforcing functional specification
	ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1: Delivery procedures
	ALC_FLR.2: Flaw remediation
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
ATE: Tests	ATE_COV.1: Evidence of coverage
	ATE_FUN.1: Functional testing
	ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

EAL2 Augmented with ALC_FLR.2 Assurance Components

6. TOE Summary Specification

This chapter provides an overview of the TOE operations and describes the security functions:

- Security Audit
- Cryptographic support
- User Data Protection
- Identification and Authentication
- Security Management
- Resource Utilization
- TOE Access
- Protection of the TSF

6.1 Security Audit

The TOE generates audit records for all administrator login and logoff events, policy changes, and configuration changes. The TOE Audit Log records contain the following information:

	Description

Action ID	ID number of the action. You can quickly jump to an Audit Log action by entering the ID number in the Find Action ID field and clicking Find.
Date & Time	Date and time the action occurred.
Administrator	Name and user name of the administrator that initiated the action.
Access Role	Role of the administrator.
Topic	You can filter the Audit Log by topic types. • Administration - Displays actions performed by administrators during the designated period, such as adding a new access role or configuring user directories. Also displays actions made on administrators, such as adding a new administrator or changing an administrator's permissions. • Log on/Log out - Displays log on and log out actions so you know which administrators where active during the designated period. • Status - Displays actions performed on status reports and logs, such as deleting an entry or creating an audit record. • Policy management - Displays actions performed on policies, such as updating predefined policies, editing quick policies, or creating a new policy. • Reporting - Displays actions performed on reports during the designated period, such as editing or creating a new report. • Incident management - Displays actions performed on incidents, such as deleting incidents. • Archiving - Displays actions performed on incident archives, such as deleting or restoring an archive. System modules - Displays actions performed on system modules, such as editing a configuration or adding a module.
Action Performed	Description of the action performed by the administrator—for example, "exported DLP incident to PDF file".
Details	Additional information about the action. For example, for an action such as adding a policy, rule, or exception, this shows the policy, rule, or exception name. For actions such as previewing or exporting a report, it includes the report name.
Modified Item	Identifies the object that was changed, added, or deleted. For actions performed on incidents (e.g., viewing incident details), it includes the incident ID. For report generation, it includes a task number. Click the link to view additional details.

Audit Record Content

The TOE provides a set of web interfaces that administrators can use to view the recorded audit logs. The Audit Log can be viewed via Forcepoint Security Manager GUI by Super Administrators and System Administrators.

The TOE has an internal hardware clock that provides reliable timestamps for the TOE. These timestamps are used when recording events in the audit log.

TOE Security Functional Requirements Satisfied: FAU_GEN_EXT.1, FAU_SAR.1, FAU_SAR.2.

6.2 Cryptographic Support

The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions.

Forcepoint's C Cryptographic Module is used on all platforms and operating systems. The TOE uses version 2.0.5 of this module, which received Cryptographic Module Validation Program (CMVP) certificate #2875. All communications between TOE endpoints and servers are encrypted using this module. When the endpoint communicates with the endpoint server, it negotiates the secure connection using a FIPS 140-2 approved algorithm as dictated by the server. The use of TLS v1.2 is enforced in endpoint-to server communication.

Typically, the algorithm of choice for endpoint-to-server communication is AES-256. However, the endpoint server with which the endpoint communicates via HTTPS is configured with the following encryption string, which means that the endpoint can FIPS 140-2 and Forcepoint DLP use any of these encryption protocols to encrypt communication with the server (depending on how the endpoint server responds to the endpoint's initial communication):

- TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL

Cryptographic key generation, encryption, hashing and signature services are all done with Cryptographic Algorithm Validation Program (CAVP) validated cryptography. The C Cryptographic Module has the following CAVP certificates:

- AES: #2234, #3264 and #4401
- CVL: #36, #472 and #1110
- DRBG: #264, #723 and #1419
- DSA: #693, #933 and #1176
- ECDSA: #347, #620 and #1058
- HMAC: #1363, #2063 and #2925
- RSA: #1145, #1664 and #2381
- SHS: #1923, #2702 and #3628
- 3DES: #1398, #1853 and #2373

Additionally, the TOE uses the Forcepoint Java Cryptographic Module on Windows based servers such as FSM. The Java Cryptographic Module is used on the server side to protect communications between FSM and operator workstations. The different communication configurations allow the Forcepoint Security Manager to negotiate a variety of FIPS 140-2 approved algorithms and support different versions of Web browsers that might be running on a machine from which the user is accessing the FSM.

The TOE uses version 3.0.1 of the Java Cryptographic Module, which received CMVP Certificate #3113. Cryptographic key generation, encryption, hashing and signature services are all done with Cryptographic Algorithm Validation Program (CAVP) validated cryptography. The Java Cryptographic Module has the following CAVP certificates:

- AES: #4702
- CVL: #1342, #1343, #1344 and #1345
- DRBG: #1600
- DSA: #1244
- ECDSA: #1160
- HMAC: #3114
- KAS: #130
- RSA: #2562
- SHA-3: #24
- SHS: #3849
- 3DES: #2494

TOE Security Functional Requirements Satisfied: FCS_CKM.1, FCS_CKM.4, FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d)

6.3 User Data Protection

6.3.1 Internet Access Protection

The TOE enforces an Internet Filtering Policy on controlled traffic. The policy allows administrators to define categories of websites and protocols that internal users should be prevented from accessing. Administrators specify the category and protocol restrictions to implement for each user or group of users. User traffic can be controlled in various ways, including allowing access to content, blocking access to content, or enforcing various quotas and bandwidth restrictions.

Policies are based on categories of web content and non-web protocols. Default content categories include adult material, political, business and economy, and many more. Administrators can define policies with these default categories or create new categories to create more customized policies. Default protocol categories include instant messenger, bit torrent, and many others. Like with content categories, administrators can define custom protocol categories to help enforce more customized policies.

Policies detail which filters are to be applied for web protection. Each filter includes:

- The filter type (category filter, limited access filter, or protocol filter)
- The filter name and description
- The filter contents (categories or protocols with actions applied, or a list of sites permitted)
- The number of policies that enforce the selected filter
- Actions for the filter are specified when the filter is created using the Action Buttons:

Filter Type	Action Buttons
Category filter	Use the **Permit**, **Block**, **Confirm**, or **Quota** button to change the action applied to the selected categories. To change the action applied to a parent category and all of its subcategories, first change the action applied to the parent category, and then click **Apply to Subcategories**. To enable keyword blocking, file type blocking, or blocking based on bandwidth, click **Advanced**.
Limited access filter	Use the **Add Sites** and **Add Expressions** button to add permitted URLs, IP addresses, or regular expressions to the filter. To remove a site from the filter, mark the check box next to the URL, IP address, or expression, and then click **Delete**.
Protocol filter	Use the **Permit** or **Block** button to change the action applied to the selected protocols. To change the action applied to all protocols in a protocol group, change the action applied to any protocol in the group, and then click **Apply to Group**. To log data for the selected protocol, or to enable blocking based on bandwidth, click **Advanced**.

Actions for TOE Filter Types

The scanning performed to applied the internet protection policies includes use of the Forcepoint ACE (Advanced Classification Engine) to identify malicious lures, exploit kits, emerging threats, botnet communications and other advanced threat activity. Multiple real-time content engines analyse full web page content, active scripts, web links, contextual profiles, files (including executables).

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACF.1(a)

6.3.2 Data Loss Prevention

The TOE enforces a Data Loss Prevention policy to protect an organization from information leaks and data loss both at the perimeter and inside the organization. The Forcepoint DLP component can operate alone in the network, or it can be paired with Forcepoint Web Security or Forcepoint Email Security to provide a well-rounded data loss prevention solution. The Forcepoint Web Security DLP module prevents data loss over Web channels such as HTTP, HTTPS, and FTP. The Email DLP module prevents data loss through email.

The DLP policy engine is responsible for parsing data and using analytics to compare it to the rules in the configured policies. Policies can be used to define:

- Who can move and receive data
- What data can and cannot be moved
- Where the data can be sent
- How the data can be sent
- What action to take in case of a policy breach

There are 5 kinds of DLP policies:

1. Email policy. A single email DLP policy can be defined that contains all attributes to be monitored in inbound and outbound messages. For each attribute (for example, the appearance of a defined key phrase), the policy defines whether to permit or quarantine the message, and whether a notification should be sent.
2. Web policy. A single Web DLP policy can be enabled that contains all attributes to be monitored in HTTP, HTTP, and FTP channels, and also specifies websites to which sensitive data cannot be sent.
3. Mobile policy. A single mobile DLP policy can be enabled that contains all attributes to be monitored in email being sent to users' mobile devices. For each attribute (for example, the appearance of a defined key phrase), the policy defines whether to permit or quarantine the message, and whether a notification should be sent.
4. Predefined policy. Forcepoint On-Premise Security DLP comes with a rich set of predefined policies that cover the data requirements for a wide variety of organizations. They include:
    - Acceptable use policies, such as cyberbullying, obscenities, and indecent images.
    - Content protection policies, such as Password Dissemination, Credit Cards, and Financial Information.
    - Regulations, compliance, and standards policies, such as PCI and federal regulations.
    - Data theft indicator policies, such as Suspected Malicious Dissemination and Disgruntled Employee.
5. Custom policy. This provides the ability for administrators to create custom policies specific to the needs of their organisation.

The severity and action to be taken when policy rules are matched can be managed by the administrator. The administrator can define whether incidents should be triggered every time a rule is matched or for the accumulation of matches for a particular source over time (Drip DLP), and also define how matches are counted, the threshold for triggering the incident, the severity to assign breaches, and the action plan to apply.

The TOE has 2 databases for incident and forensics data:

- The incident database contains information about policy breaches, such as what rule was matched, how many times, what were the violation triggers, what was the date, channel, source, ID, and more.
- The forensics repository contains information about the transaction that resulted in the incident, such as the contents of an email body: From:,To:, Cc: fields; attachments, file name, etc.

On Windows endpoints the TOE also supports integration with Boldon James's classification tagging system. This adds support for applying customized data tags to files on endpoints with the appropriate API installed.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(b), FDP_ACF.1(b)

6.3.3 Email Protection

The TOE enforces an email policy to provide protection for email systems to prevent malicious threats from entering an organization's network. Each message is processed by a robust set of antivirus and antispam analytics to prevent infected email from entering the network. Domain and IP address based message routing ensures reliable, accurate delivery of email.

Three types of policies are available, depending on the direction of the email—inbound, outbound, or internal. Message direction is determined on the basis of an organization's protected domains:

- Inbound - The sender address is not from a protected domain, and the recipient address is in a protected domain
- Outbound - The sender address is from a protected domain, and the recipient address is not in a protected domain
- Internal - Both the sender and recipient addresses are in a protected domain.

Policies can also be applied to outbound email communications to protect against the loss of sensitive data. The monitoring of outbound emails includes the following:

- Drip DLP monitoring (see section 6.3.2 above) to identify where sensitive data is leaked in small quantities over time.

Email messages can be managed on the basis of:

- **Message properties**: including volume, invalid recipient settings, archive message options, message sender verification, enabling Bounce Address Tag Verification (BATV)
- **Connection options**: using real-time blacklists, reverse DNS verification, reputation service, delaying SMTP greeting, enabling SMPT VRFY command, changing SMTP port)
- **True source IP detection**: using message header information and the number of network hops to an email appliance to determine the IP address of the first sender outside the network perimeter)
- **TLS connections**: forcing connections to or from a specific IP or domain group use mandatory Transport Layer Security (TLS) and determine the security level used by that connection)
- **Directory harvest attacks**: limiting the maximum number of messages and connections coming from an IP address over a given time period
- **Relay control options**: limit the domains and IP address groups for which the server is allowed to relay mail
- **Delivery Routes**: Change the order of a user directory- or domain-based route
- **Rewriting email and domain addresses**: specify recipient address rewrite entries for messages to mask address details and redirect message delivery.
- **URL Sandbox**: real-time analysis of uncategorized URLs that are embedded in inbound email

TOE Security Functional Requirements Satisfied: FDP_ACC.1(c), FDP_ACF.1(c)

6.4 Identification and Authentication

6.4.1 Administrators

The TOE requires administrators to identify and authenticate themselves with the TOE before gaining access to any of the management functionality available via the web interface or CLI once the TOE is deployed. (The installation CLI is only available when configuring the appliance prior to deployment by directly connecting to the serial port or monitor and keyboard ports on the appliance and does not require administrators to be identified and authenticated when accessing it. This is because it is assumed that an administrator has already been granted physical access to the appliance and identification and authentication is enforced at the CLI once installation has been completed.)

Administrators connect to the Forcepoint Security Manager, and are prompted to enter their authentication credentials before access to the Forcepoint Security Manager is permitted. Successful authentication to the Forcepoint Security Manager provides single sign-on to all On-Premise Security consoles. The TOE maintains a list of administrator usernames, group membership, and passwords for each administrative account, thereby authenticating access to the relevant On-Premise Security console for the administrator. TOE management through FSAM GUI is done using the Appliance Controller API.

Administrative users can be authenticated with a username and password or with an X.509 certificate. Multiple certificates can be supported for each user, as well as multiple Certificate Authorities (CAs) for signing certificates.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.1, FIA_UID.1.

6.4.2 Users

Depending on the web policy applied, unprivileged users are able to browse the internet anonymously. This web traffic is recorded with unknown user identity and the traffic is attributed based on the client IP address. Identification and authentication can be specified in email and web policies, requiring unprivileged users to identify and authenticate themselves before accessing content through the TOE, such as internet browsing or access to email account

Email users have to identify and authenticate themselves to the TOE before they are able to manage their quarantined email messages through the PEM interface provided by Forcepoint Email Security.

TOE Security Functional Requirements Satisfied: FIA_UAU.2, FIA_UID.2.

6.5 Security Management

The TOE provides a web interface that administrators can use to manage all TOE settings, policies, audit logs, administrator accounts, and user accounts. Administrators are able to access management functionality through a series of screens provided by UI framework contain text boxes, radio buttons, dropdown menus, toggle switches, etc, and Adobe Flash elements for the Dashboard. When managing policy rules, administrators can specify alternative values for the default permissive values assigned to the TOE.

Except when in monitoring only mode (in the Forcepoint Web Security module) administrators are logged out of the web interface after a period of twenty two minutes of inactivity.

The roles supported by the Forcepoint Security Manager infrastructure are:

- Global Security Administrator- this role has permissions to perform all actions in all modules.
- Conditional Super Administrator – this role has the ability to create administrators with the module the role is associated.
- Delegated Administrator – the only Forcepoint Security Manager permission this role has is to reset their password. The role has all permissions within the module it is associated.

Delegated administrators are given access to one or more On-Premise Security consoles (Web, Data, Email). They can also be granted access to the one or more Content Gateway Manager instances. The permissions these administrators have in each On-Premise Security Console depend on which Delegated Administrator Role is assigned to the administrators. The TOE maintains nine roles for Delegated Administrators, as detailed in the table in section 5.2.5.9.

A Global Security Administrator is a user with equivalent Super Administrator access to all On-Premise Security modules (Web Security, Data Security, and Email Security). Only Super Administrators will policy or higher permissions can review the audit data (audit data is distinct from the reports of user incidents that can be reviewed by Reporting Administrators, System Administrators and Group Reporting Administrators, as well as Super Administrators).

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3(a), FMT_MSA.3(b), FMT_MSA.3(c), FMT_MTD.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1.

6.6 Resource Utilization

The TOE is capable of limiting access of users to a set of content based on a time limit quota. When the user's time quota has been used up, the TOE then blocks all attempts the user makes to access content within those controlled categories. An example of how this might be used is to allow users an hour each day to browse content that is non-conducive to productivity (such as streaming video sites) without completely restricting the content.

The TOE is capable of limiting the allocation of network bandwidth to a list of categories. Administrators define a threshold that the set of categories should not exceed. If the threshold is reached or exceeded for the overall bandwidth usage for a given user for the set of categories, any future attempts by the user to establish a connection via the set of categories are blocked by the TOE until more bandwidth becomes available.

TOE Security Functional Requirements Satisfied: FRU_RSA.1(a), FRU_RSA.1(b).

6.7 TOE Access

The TOE is capable of limiting the number of concurrent sessions users can have based on available bandwidth. If a user attempts to establish a new concurrent session while the bandwidth threshold for that type of traffic is met or exceeded, the TOE will block the new session from being established.

The web interface enforces a hard-coded twenty two minute timeout period for administrative sessions. If an administrator is inactive while logged into the web interface for twenty two minutes, the TOE terminates the session and the administrator must log in again.

TOE Security Functional Requirements Satisfied: FTA_MCS.2, FTA_SSL.3.

6.8 Protection of the TSF

Communications to the Forcepoint DLP Endpoint client devices, from the Secondary Forcepoint DLP Server, are transmitted over HTTPS connections. Communications can include Forcepoint DLP policies to be implemented at the client device and actions taken at the client device as a result of policy application. The messages are transferred via HTTPS. The TOE protects these transmissions between the Secondary Forcepoint DLP server component and the Forcepoint DLP Endpoint client device from disclosure and modification by encrypting the transmissions using TLS, as described in Section 6.2. Cryptographic services are provided by Forcepoint's FIPS certified cryptographic module. Encryption is applied by default to all communication between the client and server in the evaluated configuration. Session keys will be released from memory when the session is terminated.

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

7. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Requirement Dependencies
- TOE Summary Specification.

7.1 Security Objectives Rationale

7.1.1 Security Objectives Rationale Relating to Policies

This section shows that all secure usage assumptions and threats are completely covered by security objectives for the TOE or operational environment. In addition, each objective counters or addresses at least one assumption or threat.

	T.EXTERNAL_CONTENT	**T.DATA_LOSS**	**T. MASQUERADE**	**T.NACCESS**	**T.UNAUTHORIZED_ACCESS**	**T.RESOURCE**	**A.INSTALL**	**A.NETWORK**	**A.LOCATE**	**A.NOEVIL**	**A.MANAGE**
O.AUTHENTICATE			X		X						
O.AUDIT					X						
O.MANAGE					X						
O.RESOURCE_CONTROL	X										
O.DATA_PROTECT		X									
O.QUOTA						X					
O.TIMESTAMP					X						
O.HARMFUL_CONTENT	X			X							
O.PROTECT					X						
OE.NETWORK								X			
OE.PROTECT				X	X						
OE.CLIENT					X						
OE.ADMIN							X			X	X
OE.USER										X	
OE.LOCATE									X		

Security Problem Definition to Security Objective Correspondence

The following tables provide detailed evidence of coverage for each threat, policy, and assumption:

THREATS	OBJECTIVES	RATIONALE
T.EXTERNAL_CONTENT **Error! Reference source not found.**	O.RESOURCE_CONTROL **Error! Reference source not found.**	O.RESOURCE_CONTROL counters this threat by ensuring that network resources controlled by the policies can be blocked when they contain potentially harmful or inappropriate content.
	O.HARMFUL_CONTENT The TOE must disallow access to malicious content hidden within legitimate network resource requests.	O.HARMFUL_CONTENT counters this threat by ensuring that malicious content is removed from trusted content prior to being delivered to the internal network, thereby minimizing the risk of attack to the internal network.
T.DATA_LOSS **Error! Reference source not found.**	O.DATA_PROTECT **Error! Reference source not found.**	O.DATA_PROTECT counters this threat by ensuring all content is inspected before it is transmitted outside the organization taking

THREATS	OBJECTIVES	RATIONALE
		specified actions to ensure sensitive files and data are not released counter to the configured policy.
T.MASQUERADE A user may masquerade as another entity in order to gain unauthorized access to user data or On-Premise Security controlled resources.	O.AUTHENTICATE **Error! Reference source not found.**	O.AUTHENTICATE counters this threat by ensuring that TOE administrators and users supply login credentials before being granted access to services or information, thereby reducing the risk of access by masquerading.
T.NACCESS An unauthorized person or external IT entity may be able to view or modify On-Premise Security configuration and control data by hijacking an unattended administrator session.	O.PROTECT The TOE must have the capability to protect configuration data from unauthorized reading or modification.	O.PROTECT help mitigate this threat by ensuring that unattended management sessions do not permit attackers to access management functionality.
	OE.PROTECT The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE components, between the Forcepoint Security Manager and the administrator, and between TOE components and (optional) authentication server.	OE.PROTECT further mitigates this threat by ensuring the IT environment provides protection of the communication between the TOE components, between the Forcepoint Security Manager and the administrator, and between TOE components and (optional) authentication server.
T.UNAUTHORIZED_ACCESS A user may gain access to security data controlled by On-Premise Security that they are not authorized to access.	O.AUTHENTICATE **Error! Reference source not found.**	O.AUTHENTICATE counters this threat by ensuring that users supply login credentials before being granted access to any security-relevant information.
	O.AUDIT **Error! Reference source not found.**	O.AUDIT counters this threat by ensuring that the TOE records potential security breaches and suspicious activity, and allows authorized administrators to review this activity.
	O.MANAGE **Error! Reference source not found.**	O.MANAGE counters this threat by providing the capability for an administrator to properly configure the management mechanisms of the TOE designed to mitigate this threat.
	O.TIMESTAMP The TOE must provide a timestamp for its own use.	O.TIMESTAMP counters this threat by ensuring that timestamps used in the audit records created by O.AUDIT are reliable. These audit records are used by administrators to observe any suspicious activity.
	O.PROTECT The TOE must have the capability to protect configuration data from unauthorized reading or modification.	O.PROTECT helps to mitigate this threat by ensuring that the TOE is capable of protecting management data and access to management functionality from unauthorized access via an unattended management session.

THREATS	OBJECTIVES	RATIONALE
	OE.PROTECT The IT environment must protect itself and the TOE from external interference or tampering, and must protect the communication between the TOE components, between the Forcepoint Security Manager and the administrator, and between TOE components and (optional) authentication server.	OE.PROTECT also helps to mitigate this threat by ensuring the IT environment provides protection of the communication between the TOE components, between the Forcepoint Security Manager and the administrator, and between TOE components and (optional) authentication server.
	OE.CLIENT The endpoint client workstations must be logically protected using best practices, including the installation of anti-virus and anti-spyware software and configuration of PC firewall.	OE.CLIENT further mitigates this threat by ensuring the IT environment provided by the endpoint client workstation is protected by best security practices to protect against logical attack against the TOE endpoint component.
T.RESOURCE On-Premise Security users or attackers may cause network connection resources to become overused and therefore unavailable.	O.QUOTA The TOE must be able to place quotas on network connection resources.	O.QUOTA counters this threat by ensuring that the TOE is capable of placing administrator-defined quotas on the network resources, thereby ensuring that those resources do not become unavailable.

Threats to Objectives Mapping Rationale

ASSUMPTIONS	OBJECTIVES	RATIONALE
A.INSTALL On-Premise Security has been installed and configured according to the appropriate installation guides.	OE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	OE.ADMIN upholds this assumption by ensuring that the administrator responsible for On-Premise Security installs and configures On-Premise Security according to the guidance documentation.
A.NETWORK **Error! Reference source not found.**	OE.NETWORK All policy-controlled protocol traffic between the internal and external network must traverse the TOE.	OE.NETWORK upholds this assumption by ensuring that the IT environment is configured such that no policy-controlled traffic can travel between the internal and external networks without traversing On-Premise Security.
A.LOCATE **Error! Reference source not found.**	OE.LOCATE The physical environment must be suitable for supporting computing devices in a physically secure setting.	OE.LOCATE upholds this assumption by ensuring that the IT environment is suitable to ensure the proper, secure functioning of the On-Premise Security components and protects the communication between the On-Premise Security components, between the Forcepoint Security Manager and the administrator and between the On-Premise Security components and (optional) authentication server.
A.NOEVIL It is assumed that administrators who manage On-Premise	OE.ADMIN The administrator must not be careless, negligent, or willfully	OE.ADMIN helps to uphold this assumption by ensuring that administrators are non-hostile,

ASSUMPTIONS	OBJECTIVES	RATIONALE
Security are not careless, negligent, or willfully hostile; are appropriately trained; and follow all guidance.	hostile; must be appropriately trained; and must follow all guidance.	appropriately trained and follow all administrator guidance.
	OE.USER The Authorized users are trusted to not actively or negligently compromise the security of the component on which the TOE Endpoint component is installed.	OE.USER further upholds this assumption by ensuring that users are non-hostile and follow best security practice.
A.MANAGE There are one or more competent individuals assigned to manage On-Premise Security and the security of the information it contains.	OE.ADMIN The administrator must not be careless, negligent, or willfully hostile; must be appropriately trained; and must follow all guidance.	OE.ADMIN upholds this assumption by ensuring that those responsible for On-Premise Security provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use.

Assumptions to Objectives Mapping Rationale

7.2 Security Functional Requirements Rationale

All security functional requirements identified in this Security Target are fully addressed in this section and each is mapped to the objective it is intended to satisfy. The table below summarizes the correspondence of functional requirements to TOE security objectives.

	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.RESOURCE_CONTROL	O.DATA_PROTECT	O.QUOTA	O.TIMESTAMP	O.HARMFUL_CONTENT	O.PROTECT
FAU_GEN_EXT.1	X								
FAU_SAR.1	X								
FAU_SAR.2	X								
FCS_CKM.1									X
FCS_CKM.4									X
FCS_COP.1(a)									X
FCS_COP.1(b)									X
FCS_COP.1(c)									X
FCS_COP.1(d)									X
FDP_ACC.1(a)				X				X	
FDP_ACC.1(b)					X				
FDP_ACC.1(c)					X				
FDP_ACF.1(a)				X				X	
FDP_ACF.1(b)					X				
FDP_ACF.1(c)					X				
FIA_ATD.1		X							

	O.AUDIT	O.AUTHENTICATE	O.MANAGE	O.RESOURCE_CONTROL	O.DATA_PROTECT	O.QUOTA	O.TIMESTAMP	O.HARMFUL_CONTENT	O.PROTECT
FIA_UAU.1		X							
FIA_UAU.2		X							
FIA_UID.1		X							
FIA_UID.2		X							
FMT_MOF.1			X						
FMT_MSA.1(a)			X	X				X	
FMT_MSA.1(b)			X		X				
FMT_MSA.3(a)			X	X				X	
FMT_MSA.3(b)			X		X				
FMT_MSA.3(c)			X		X				
FMT_MTD.1	X								
FMT_SAE.1									X
FMT_SMF.1			X						
FMT_SMR.1			X						
FPT_STM.1							X		
FPT_ITT.1									X
FRU_RSA.1(a)						X			
FRU_RSA.1(b)						X			
FTA_MCS.2			X						
FTA_SSL.3									X

Objective to Requirement Correspondence

O.AUDIT

The TOE must record events of security relevance at the "not specified" level of audit. The TOE must record system configuration and traffic policy updates and allow trained administrators to review security-relevant audit events.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN_EXT.1: The TOE must generate audit records at the "not specified" level of audit. These records must contain data such as time and date information, IP addresses and user identity information.
- FAU_SAR.1: The TOE must provide administrators access to audit events.
- FAU_SAR.2: The TOE must only allow authorized administrators and users to view audit records.
- FMT_MTD.1: The TOE must only allow authorized administrators to manage audit data.

O.AUTHENTICATE

The TOE must require the administrator to authenticate before gaining access to the administrative interfaces of the TOE and users to authenticate if their network request matches a traffic policy rule that requires user authentication. The TOE must require the PEM user to authenticate before gaining access to the user's quarantined email.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE must be able to maintain a list of security attributes used for administrator authentication.
- FIA_UAU.1: Administrators must authenticate their identities before being allowed access to any TOE management functionality besides the installation CLI.
- FIA_UAU.2: Users must authenticate their identities before gaining access to network resources.
- FIA_UID.1: Administrators must identify themselves before being allowed access to any TOE management functionality besides the installation CLI.
- FIA_UID.2: Users must identify themselves before being allowed access to network resources.

O.MANAGE

The TOE must provide secure management of the system configuration and the traffic policies over one or more concurrent sessions.

- FMT_MOF.1: TOE management activities available to each administrative role are specified.
- FMT_MSA.1(a), (b): Administrative roles which can manage security attributes related to network policies are specified.
- FMT_MSA.3(a), (b), (c): The default security posture of the network policies and administrative roles that can change the policy from the default policy are specified.
- FMT_SMF.1: The management functionality available for the TOE is specified.
- FMT_SMR.1: The roles that are available for administrators are specified. The proper association of administrators with assigned roles is also required.
- FTA_MCS.2: Administrators must be able to manage and define the number of concurrent sessions that an end user can run.

O.RESOURCE_CONTROL

The TOE must control access to network resources as defined by the traffic policies.

- FDP_ACC.1(a): The TOE must be able to control access of subjects (users) to objects (external IT entities hosting content).
- FDP_ACF.1(a): The TOE must be able to utilize the attributes of the controlled network traffic to enforce the Internet Access Policy.
- FMT_MSA.1(a): Only authorized administrators can modify security attributes associated with the Internet Access Policy.
- FMT_MSA.3(a): The Internet Filtering Policy is permissive by default, and only authorized administrators can modify this default posture.

O.DATA_PROTECT

The TOE will take specified actions against transmission of identified files or data.

- FDP_ACC.1(b): the TOE must be able to control access of subjects (users) to objects (filesystem files, email messages, database entries).
- FDP_ACC.1(c): The TOE must be able to control access of subjects (users) to objects (email messages).
- FDP_ACF.1(b): The TOE must be able to utilize the attributes of the controlled network traffic to enforce the Data Loss Prevention Policy.
- FDP_ACF.1(c): The TOE must be able to utilize the attributes of the controlled email traffic to enforce the Email Policy.

- FMT_MSA.1(b): Only authorized administrators can modify security attributes associated with the Data Loss Prevention Policy.
- FMT_MSA.3(b): The Data Loss Prevention Policy must be permissive by default, and only authorized administrators can modify this default posture.
- FMT_MSA.3(c): The Email Policy must be permissive by default, and only authorized administrators can modify this default posture.

O.QUOTA

The TOE must be able to place quotas on network connection resources.

- FRU_RSA.1(a): The TOE must be capable of placing maximum quotas on the number of connections available during a specified time period.
- FRU_RSA.1(b): The TOE must be able to place maximum quotas on the bandwidth available for use by different types of traffic.

O.TIMESTAMP

The TOE must provide a timestamp for its own use.

- FPT_STM.1: The TOE must be able to provide timestamps for its own use.

O.HARMFUL_CONTENT

The TOE must disallow access to malicious content hidden within legitimate network resource requests.

- FDP_ACC.1(a): The Internet Filtering Policy must be able to block harmful content that might exist within trusted content.
- FDP_ACF.1(a): the TOE must be able to utilize the attributes of the controlled network traffic to enforce the Internet Filter Policy.
- FMT_MSA.1(a): Only authorized administrators can modify security attributes associated with the Proxy Filtering Policy.
- FMT_MSA.3(a): The Internet Filtering Policy must be permissive by default, and only authorized administrators can modify this default posture.

O.PROTECT

The TOE must have the capability to protect configuration data from unauthorized reading or modification.

- FCS_CKM.1: Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FCS_CKM.4: Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FCS_COP.1(a): Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FCS_COP.1(b): Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FCS_COP.1(c): Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FCS_COP.1(d): Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FMT_SAE.1: Authorized administrators must be able to monitor real-time updated data pages without risking an unauthorized individual gaining access to an unattended management session.

- FPT_ITT.1: Data exchanged between the Secondary Data server and Forcepoint DLP Endpoint client must be protected.
- FTA_SSL.3: unauthorized individuals must not be able to gain access to the TOE through an unattended management session.

7.3 Security Assurance Requirements Rationale

The security assurance requirements for the TOE are the EAL 2 augmented with the ALC_FLR.2 component as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

EAL 2 augmented with ALC_FLR.2 was selected as the assurance level because the TOE is a commercial product whose users require a low to moderate degree of independently assured security. ALC_FLR.2 was selected to exceed EAL2 assurance objectives in order to ensure that identified flaws are addressed. The TOE is targeted at a relatively benign environment with good physical access security and competent administrators. Within such environments it is assumed that attackers will have little attack potential. As such, EAL 2 augmented with ALC_FLR.2 is appropriate to provide the assurance necessary to counter the limited potential for attack.

7.4 Requirements Dependency Rationale

The following table identifies the SFRs claimed in the ST, their dependencies as defined in CC Part 2, and how the dependency is satisfied in the ST. It can be seen that all dependencies have been satisfied by inclusion in the ST of the appropriate dependent SFRs.

Requirement	Dependencies	How Satisfied
FAU_GEN_EXT.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN_EXT.1
FAU_SAR.2	FAU_SAR.2	FAU_SAR.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1
	FCS_CKM.4	FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
FCS_COP.1(*)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	FCS_CKM.4
FDP_ACC.1(*)	FDP_ACF.1	FDP_ACF.1(*)
FDP_ACF.1(*)	FDP_ACC.1	FDP_ACC.1(*)
	FMT_MSA.3	FMT_MSA.3(*)
FIA_ATD.1	None	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1	FIA_UID.1
FIA_UID.1	None	n/a
FIA_UID.2	None	n/a
FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1(*)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1(*)
	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3(*)	FMT_MSA.1	FMT_MSA.1(*)
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
	FMT_SMR.1	FMT_SMR.1
FMT_SAE.1	FMT_SMR.1	FMT_SMR.1
	FPT_STM.1	FPT_STM.1

Requirement	Dependencies	How Satisfied
FMT_SMF.1	None	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	None	n/a
FPT_ITT.1	None	n/a
FRU_RSA.1(*)	None	n/a
FTA_MCS.2	FIA_UID.1	FIA_UID.1
FTA_SSL.3	None	n/a

Requirement Dependencies

7.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. The following table demonstrates the relationship between security requirements and security functions.

	Security Audit	Cryptographic support	User Data Protection	Identification and Authentication	Security Management	Protection of TOE Security Functions	Resource Utilization	TOE Access
FAU_GEN_EXT.1	X							
FAU_SAR.1	X							
FAU_SAR.2	X							
FCS_CKM.1		X						
FCS_CKM.4		X						
FCS_COP.1(a)		X						
FCS_COP.1(b)		X						
FCS_COP.1(c)		X						
FCS_COP.1(d)		X						
FDP_ACC.1(a)			X					
FDP_ACF.1(a)			X					
FDP_ACC.1(b)			X					

	Security Audit	Cryptographic support	User Data Protection	Identification and Authentication	Security Management	Protection of TOE Security Functions	Resource Utilization	TOE Access
FDP_ACF.1(b)			X					
FDP_ACC.1(c)			X					
FDP_ACF.1(c)			X					
FIA_ATD.1				X				
FIA_UAU.1				X				
FIA_UAU.2				X				
FIA_UID.1				X				
FIA_UID.2				X				
FMT_MOF.1					X			
FMT_MSA.1(a)					X			
FMT_MSA.1(b)					X			
FMT_MSA.3(a)					X			
FMT_MSA.3(b)					X			
FMT_MSA.3(c)					X			
FMT_MTD.1					X			
FMT_SAE.1					X			
FMT_SMF.1					X			
FMT_SMR.1					X			
FPT_STM.1						X		
FRU_RSA.1(a)							X	
FRU_RSA.1(b)							X	
FTA_MCS.2								X
FTA_SSL.3								X
FPT_ITT.1						X		

Security Functions vs. Requirements Mapping