Everfox LLC

Data Guard

v4.0.0.2

Security Target

Evaluation Assurance Level (EAL): 4+
Document Version: 0.9

Prepared for:

EVERFOX

Everfox LLC.
12950 Worldgate Drive
Suite 600
Herndon, VA 20170
United States of America

Phone: +1 703 318 7134
www.everfox.com

Prepared by:

Corsec

Corsec Security, Inc.
12600 Fair Lakes Drive
Suite 210
Fairfax, VA 22033
United States of America

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Everfox Data Guard v4.0.0.2 application and will hereafter be referred to as the TOE throughout this document. The TOE is an automated data transfer guard that enables the secure movement of structured data between multiple separate domains or 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 functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 shows the ST and TOE references.

Please note: The TOE reference cannot be explicitly queried. When querying the TOE, "Forcepoint Data Guard v4.0.0.2" will be returned instead. The TOE was originally developed under the Forcepoint brand when the evaluation commenced, and has not yet been fully rebranded in all components.

Table 1 – ST and TOE References

ST Title	*Everfox Data Guard v4.0.0.2 Security Target*
ST Version	Version 0.9
ST Author	Corsec Security, Inc.
ST Publication Date	January 23, 2026
TOE Reference	Everfox Data Guard v4.0.0.2

1.3 Product Overview

Everfox Data Guard (referred to as Data Guard) is a software product designed to inspect, validate, and filter network traffic using a flexible rules engine that allows administrators to implement data protection and sharing policies for enterprise data. Data Guard supports large enterprise systems with low administration costs, making it the ideal choice for large scale government deployments that require large volume, automated data transfers. Data Guard was formerly known as "Forcepoint Data Guard" and the acronym FDG is still used for file names and to describe the CLI.

Data Guard can be configured for unidirectional or bidirectional automated data transfer to secure the flow of data between multiple, separate unclassified and classified domains or networks. Data Guard includes a Red Hat Enterprise Linux (RHEL) 8.10 secure Operating System (OS) with Security Enhanced Linux (SELinux) modules allowing it to delivers byte-level deep content inspection and data validation and filtering that can be tailored to meet security policies, requirements, and to mitigate risks specific to each customer environment.

Data Guard provides a flexible yet exhaustive capability to inspect data streams down to the byte level as required by the customer security policy. Support is provided for any data transmitted via Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) over Internet Protocol (IP). Data Guard can be managed using an ONVIF interface and REST API that are disabled by default and by both a Data Guard CLI and the RedHat CLI. A number of filtering plug-ins are also included in Data Guard.

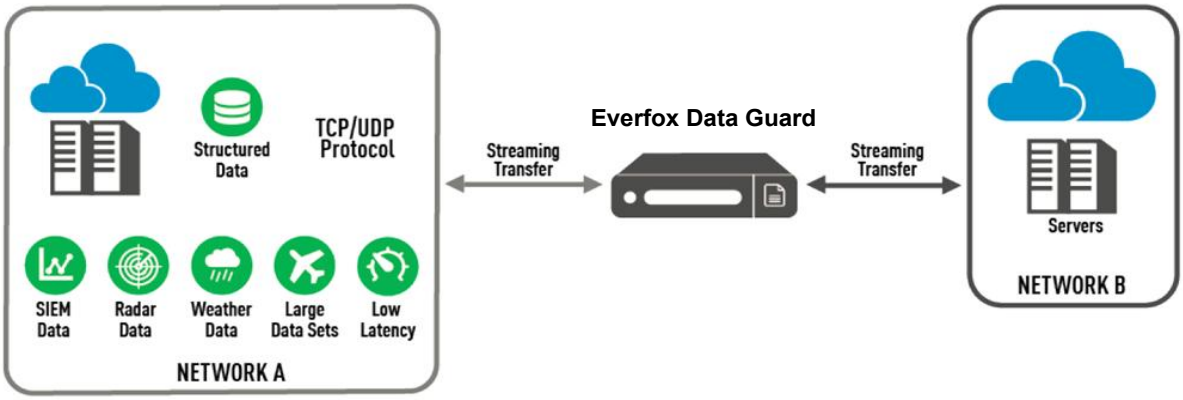

Figure 1 –TOE TCP/UDP Data Transfer Architecture

1.4 TOE Overview

The TOE is a software solution that runs on COTS[1] hardware and is deployed between domains or networks of different security or classification levels. The TOE inspects and filters transiting data flows by applying the Lua runtime filtering rules to the traffic that flows between the NPAs (Network Protocol Adapters). By default, no data can flow between the NPAs unless the rules allow the flow.

Administrators use the administrative CLI to implement rules to define unidirectional or bidirectional flow. The rules are based on the Lua scripting language. Lua rules provide flexible filtering and data validation to allow or drop a data payload from a high-level (interface, network zone, or protocol) down to the byte level for deep content inspection.

[1] COTS – Commercial Off The Shelf

The TOE generates audit records for configuration changes, successful CLI commands, flow events, and startup and shutdown of the audit function. An authorized administrator filters and views the audit records from the CLI.

An administrator can only access the TOE after the administrator is identified by the TOE and assigned the role associated with the logged in account.

1.4.1 TOE Components

The TOE software is available as an ISO image that includes the EDG 4.0 application and all its components. The TOE is separated into the following components:

- Data Flow Manager (**DFM**)
- Data Filtering Process (**DFP**)
- Inbound Network Protocol Adapter (**INPA**)
- Outbound Network Protocol Adapter (**ONPA**)

1.4.1.1 Data Flow Manager (DFM)

The **DFM** is the center point to create and monitor the filtering pipeline processes. Processes are created based on Data Flow definitions. The **DFM** starts the **INPA**, **DFP**, and **ONPA** processes and monitors the health and status of these processes. The **DFM** also provides a CLI to allow administrators control over the **DFM** and to set the configuration files for all the components.

Administrators use the TOE's CLI to configure settings such as allowing traffic to sources and destinations, applying data flow policies, and to importing the filter rules used to inspect and validate the data flows. The TOE's CLI also provides data flow management and monitoring tools to manage the startup and shutdown of filter processing and retrieval of various data flow transfer and filter statistics.

1.4.1.2 Data Filtering Process (DFP)

The **DFP** provides the core filtering capabilities for the TOE. The **DFP** handles the input/output operations for the flow data and hosts the Filtering Engine. The Filtering Engine is a customized version of the Lua v5.1.5 runtime environment, which is embedded in the TOE's software. Administrators implement rule sets written in Lua's scripting language to validate the data flowing through the Filter Engine. The Filter Engine can be used to chain multiple **DFP** filters.

The **DFP** receives data payloads from the **INPA** and applies filter rules to determine if the data should be passed or dropped. If the data passes validation, it is passed to the **ONPA**. The filter rules are constructed using Lua programming language on top of the TOE filter APIs.

1.4.1.3 Inbound Network Protocol Adapter (INPA)

The **INPA** receives traffic from the environment. The traffic originates from an external source endpoint over a UDP or TCP connection. The **INPA** extracts the data payload and checks the configured data flow policies before send any of the allowed data to the **DFP** for filtering. The configuration file for the **INPA** is updated by the **DFM** after a RW administrator makes changes from the CLI.

1.4.1.4 Outbound Network Protocol Adapter (ONPA)

The **ONPA** receives its data payload from the **DFP** and checks the configured data flow policies before sending the payload to an external destination endpoint using a UDP or TCP connection. The configuration file for the **ONPA** is updated by the **DFM** after a RW administrator makes changes from the CLI.

1.5 TOE Environment

The TOE runs on RHEL 8.10 OS, which in turn provides core services such as authentication, data storage, SSH (Secure Shell) for remote authentication, and TCP/IP networking support. The TOE runs on top of the RHEL platform using built-in modules and open-source components to provide enhanced security protection, including:

- SELinux type enforcement: Provides mandatory access control for higher assurance enforcement of process execution and separation. Access control to and from an external network is enforced based on the zone ID associated with an administrator-named zone.
- Iptables: Provides packet filtering capabilities to control inbound and outbound access to network services.

The TOE bridges communication between two separate external networks. The **INPA** receives network traffic from the external inbound network over a TCP or UDP connection and sends the traffic to the **DFP** for filtering. The **ONPA** receives the filtered data from the **DFP** and sends the data to the external outbound network over a TCP or UDP connection. Management of the TOE is performed via the CLI using either a remote SSH connection or the local console. Table 2 specifies the minimum system requirements for the proper operation of the TOE.

Table 2 – TOE Minimum Requirements

Category	Requirement
Hardware	The minimum hardware requirements include the following: • At least one network interface card • 2 CPU • 2 GB[2] of memory • 120 GB of storage See the minimum hardware requirements for RHEL 8.10 listed at https://access.redhat.com/articles/rhel-limits.
Networks	Inbound and outbound networks are required for the TOE to filter traffic.

1.6 TOE Description

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

1.6.1 Physical Scope

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all the components of the TOE.

The TOE is a software product which runs on a commercially available hardware server compliant with the minimum software and hardware requirements as listed in Table 2.

[2] GB – Gigabyte

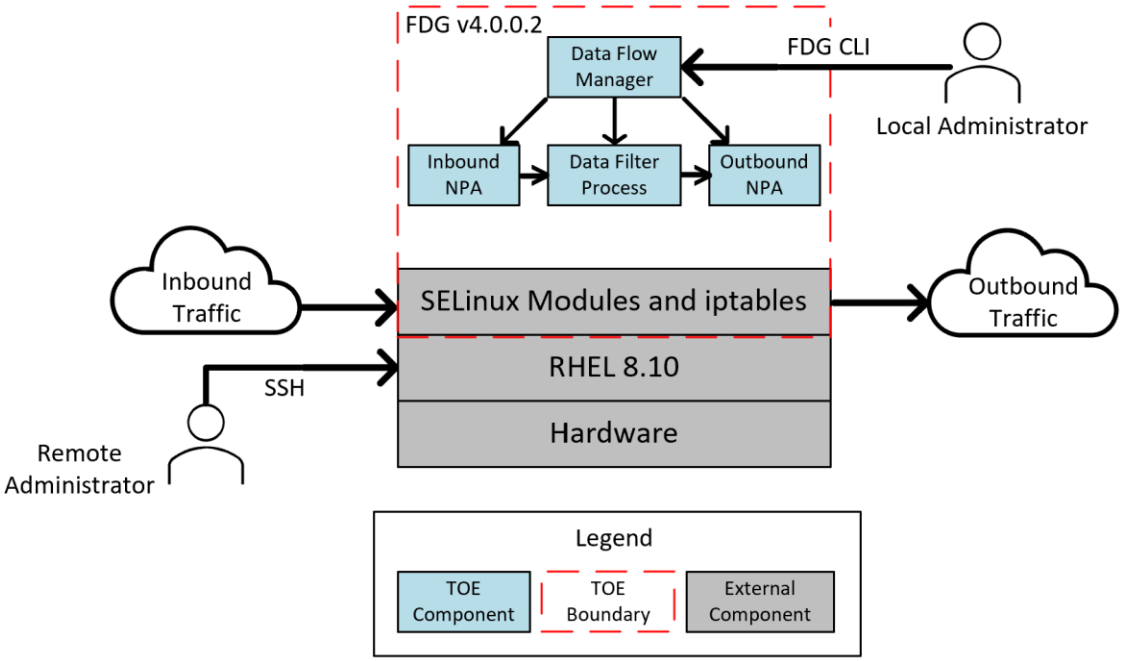

Figure 2 – Physical TOE Boundary

1.6.1.1 TOE Software

The TOE is software-only and includes the following ISO file:

- `fdg-4-0-0-2-38816-GA-2024-11-05.iso` – contains the TOE software

The Forcepoint Installation Media packet contains CDs along with a copy of the Forcepoint Software License Agreement, product cover letter, and the Forcepoint Software Maintenance Agreement (if purchased). The TOE installation ISO, fdg-4-0-0-2-38816-GA-2024-11-05.iso, contains the TOE installation files, and the TOE documentation *fdg-4-0-0-2_documentation_2024-11-05* ISO contains the TOE documentation files.

Once each ISO is copied onto a Linux system, the customer runs the following command to compute the SHA256 checksum:

sha256sum /<path to ISO file>

Checksum files are provided along with the product ISO. A checksum on the product ISO should be compared with the checksum file provided by Everfox and they should match. The customer then contacts Everfox for verification of the SHA256 checksum value. Customers should contact Everfox via email in order to obtain the TOE Guidance Supplement, delivered over Kiteworks.

1.6.1.2 Guidance Documentation

The TOE documentation ISO (`fdg_4-0-0-2_documentation_2024-11-05.iso`) contains PDF[3] of all documents except the Guidance Supplement. All are required reading and part of the TOE:

Table 3 – TOE Guidance Documentation

[3] PDF – Portable Data Format

Title	Filename	Description
Everfox (Formerly Forcepoint) Data Guard Administrator's Guide Version 4.0.0.2; November 5, 2024	`fdg_4-0-0-2_documentation_2024-11-05.pdf`	Includes steps for the installation, configuration, and maintenance of the TOE.
Everfox (Formerly Forcepoint) Data Guard Filter Development Guide Version 4.0.0.2; November 5, 2024	`fdg_4-0-0-2_filter-dev-guide_2024-11-05.pdf`	enables the development of rulesets for the DFP, including the API[4] to construct Lua filters for generic filtering
Everfox (Formerly Forcepoint) Data Guard Release Notes Version 4.0.0.2; November 5, 2024	`RELEASE_NOTES.pdf`	Provides product changes for version 4.0.0.2
Everfox Data Guard 4.0.0.2 Guidance Supplement v0.7	Everfox Data Guard 4.0.0.2 Guidance Supplement – 0.7.pdf	Everfox Guidance document for Common Criteria

The Everfox Data Guard v4.0.0.2 Guidance Supplement v0.7, is available upon request from a customer.

1.6.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management

1.6.2.1 Security Audit

Audit functionality is provided by the TOE for generation of audit records for the startup/shutdown of the audit function, configuration changes, and data flow events. From the TOE's CLI, administrators may view the following log files: `audit.log`, `xguard-admin.log` and `xguard-flow.log`.

1.6.2.2 User Data Protection

Information flow control is provided by the TOE with the INPA Information Flow SFP (INPA SFP), ONPA Information Flow SFP (ONPA SFP) and the Flow SFP. The INPA SFP controls the flow of inbound data from an external network. The ONPA SFP controls the flow of outbound data to an external network. The Flow SFP controls what is allowed to pass between the INPA and ONPA after filtering the data in the DFP. By default, no data is allowed to flow unless the flow is defined and permitted. A RW administrator defines the flow filtering rules using the Lua scripting language and imports the rules as a Lua file.

1.6.2.3 Identification and Authentication

The TOE requires administrators to be identified by their TOE roles before gaining access to any TOE data or functionality.

1.6.2.4 Security Management

The TOE provides the capability to manage the security functionality, TSF data, and security attributes of the TOE. The TOE also provides the read-only (RO) and read-write (RW) roles. The read-only role provides limited capabilities to view TSF data. The read-write role provides full administrative capabilities to manage the TSF. An administrator assigned to the RO role is referred to as a RO administrator. An administrator assigned to the RW

[4] API – Application Programming Interface

role is referred to as a RW administrator. The unqualified term “administrator,” when not preceded by RO or RW, refers to both RO administrators and RW administrators.

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

Features and/or Functionality that are not part of the evaluated configuration of the TOE are:

- ONVIF Interface (disabled by default)
- REST API (disabled by default)
- Filtering functionalities provided by the following plug-ins:
  - Glasswall Plug-in
  - McAfee Plug-In
  - XML (Extensible Markup Language) Plug-In
  - JSON (JavaScript Object Notion) Plug-In
- Functionality to implement, configure, or add the following:
  - CLI Timeout
  - Login Banner
  - File Integrity
  - Web Data Flow
  - System Alert Emails
  - Log file rotation, exportation
  - TOE backup, restoration, reset
  - PKI Certificates
  - System License
  - Set Hostname
  - Password Complexity
  - Updates to the TOE via the CLI
  - Transparent mode in flow configuration
  - NTP support
  - SNMP support
  - filedrop
  - filedrop flow
  - multi-zone DNS support
  - integration with ZTCDR
  - Deep Secure Web and Mail Guards
  - Account lockout policy

2. Conformance Claims

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

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version CC:2022, Release 1, November 2022; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	N/A
Evaluation Assurance Level	EAL4+ augmented with Flaw Remediation (ALC_FLR.2)

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 to which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel, and connectivity aspects

3.1 Threats to Security

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

- Attackers who are not TOE administrators: 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 administrators: 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 administrators are, however, assumed not to be willfully hostile to the TOE.)

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

Name	Description
T.FLOW	An attacker may try to gain access to the destination network or to data in transit to the destination network by bypassing the data flow policies placed on the networks.
T.REVERSE_FLOW	An attacker may try to gain access to the data that is sent in reply from the destination network by bypassing the data flow policies placed on the networks.
T.UNDETECTED_ACTIONS	An attacker may take actions that adversely affect the security of the TOE assets and these actions remain undetected so that their effects cannot be effectively countered.
T.UNPRIVILEGED	An underprivileged user may try to change the TOE configuration and compromise its security functions.

Table 5 – Threats

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. There are no OSPs for this ST.

[5] TSF – TOE Security Functionality

3.3 Assumptions

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

Table 6 – Assumptions

Name	Description
A.PLATFORM	The TOE is installed on the appropriate, dedicated hardware and the platform contains only the approved applications needed to support the TOE as per the installation guidance.
A.NETCON	The TOE environment provides network connectivity between the TOE and external networks.
A.TIMESTAMP	The IT environment provides the TOE with the necessary and reliable timestamps.
A.PHYSICAL	The TOE is located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.ADMIN	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators are trusted and assumed not to be willfully hostile to the TOE.
A.AUTHENTICATION	The platform that the TOE is installed on will provide adequate authentication methods for TOE administrators.

4. Security Objectives

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

4.1 Security Objectives for the TOE

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

Table 7 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must enforce an access control policy to provide appropriate access to administrators that view or manage TOE resources based on their assigned roles.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.
O.IDENTIFY	The TOE must be able to identify administrators prior to allowing access to TOE administrative functions and data.
O.FLOW	The TOE must ensure that data will flow only as defined in the Information Flow SFPs.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 8 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external access attempts or attempts to intercept the data transiting the TOE. The TOE environment must provide logical and physical security controls to protect the network resources and data at the level appropriate to the sensitivity of the data.
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. The hardware and RHEL OS with SELinux and Iptables modules are installed according to the guidance to provide the functionality necessary to support the secure operation of the TOE.
OE.NETWORK	The TOE environment must be implemented such that the TOE is logically connected to only the defined external inbound and outbound networks and to no other networks.
OE.AUTHENTICATE	The TOE environment must provide user authentication.

4.2.2 Non-IT Security Objectives

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

Table 9 – Non-IT Security Objectives

Name	Description
NOE.ADMIN	Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.

5. Extended Components

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

There are no extended SFRs and no extended Security Assurance Requirements (SAR) for the 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, selection and iteration operations to be performed on security functional requirements. All 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 bold text within brackets***].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [***underlined and italicized bold text within brackets***].
- 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	I
FAU_GEN.1	Audit data generation	✓	✓	
FAU_SAR.1	Audit review		✓	
FDP_IFC.1(a)	Subset information flow control (INPA Interface)		✓	✓
FDP_IFC.1(b)	Subset information flow control (ONPA Interface)		✓	✓
FDP_IFC.1(c)	Subset information flow control (Flow)		✓	✓
FDP_IFF.1(a)	Simple security attributes (INPA Interface)		✓	✓
FDP_IFF.1(b)	Simple security attributes (ONPA Interface)		✓	✓
FDP_IFF.1(c)	Simple security attributes (Flow)		✓	✓
FIA_UID.2	User identification before any action			
FMT_MSA.1(a)	Management of security attributes (INPA Interface)	✓	✓	✓
FMT_MSA.1(b)	Management of security attributes (ONPA Interface)	✓	✓	✓
FMT_MSA.1(c)	Management of security attributes (Flow)	✓	✓	✓
FMT_MSA.3(a)	Static attribute initialisation (INPA Interface)	✓	✓	✓
FMT_MSA.3(b)	Static attribute initialisation (ONPA Interface)	✓	✓	✓
FMT_MSA.3(c)	Static attribute initialisation (Flow)	✓	✓	✓
FMT_SMF.1	Specification of management functions		✓	
FMT_SMR.1	Security roles		✓	

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit data 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. [
   - ***Configuration changes***
   - ***Commands entered from the CLI***
   - ***Flow events***

   ].

FAU_GEN.1.2

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

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;
b. For each audit event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST, [***and the following audit fields in the log files:***
   c. ***`xguard-flow.log` and `xguard-admin.log` fields:***
      a. Severity
      b. Timestamp
      c. Hostname
      d. Component
      e. ***List of token=value pairs (which contains command arguments or flow information)***

   ]

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [***RW administrators***] with the capability to read [***all audit information***] from the audit data.

FAU_SAR.1.2

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

6.2.2 Class FDP: User Data Protection

FDP_IFC.1(a) Subset information flow control (INPA Interface)

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(a)

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

- ***Subject: INPA interface***
- ***Information: Inbound data traffic***
- ***Operations: Allow or deny the flow of controlled information to the INPA interface as defined by the INPA Information Flow SFP***

].

FDP_IFC.1(b) Subset information flow control (ONPA Interface)

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(b)

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

- ***Subject: ONPA interface***
- ***Information: Outbound data traffic and responses to inbound requests***
- ***Operations: Allow or deny the flow of controlled information from the controlled ONPA interface as defined by the ONPA Information Flow SFP.***

].

FDP_IFC.1(c) Subset information flow control (Flow)

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1(c)

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

- ***Subject: DFP***
- ***Information: Data flow between the INPA and the ONPA***
- ***Operations: Allow or deny the flow of controlled information between the controlled INPA and ONPA via the controlled DFP as defined by the Flow SFP.***

].

FDP_IFF.1(a) Simple security attributes (INPA Interface)

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

FDP_IFF.1.1(a)

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

- ***Subject – INPA Interface with security attributes:***
  - ***Network interface name***
  - ***Zone***
  - ***IP address***
  - ***Subnet mask***
- ***Information – Inbound data traffic with security attributes:***
  - ***Protocol type (UDP, TCP)***
  - ***Protocol state (UDP, TCP states: new, established)***

]

FDP_IFF.1.2(a)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [***if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the data is allowed to flow***.].

FDP_IFF.1.3(a)

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

FDP_IFF.1.4(a)

The TSF shall explicitly authorize an information flow based on the following rules: [***no explicit authorization rules***].

FDP_IFF.1.5(a)

The TSF shall explicitly deny an information flow based on the following rules: [***no data can flow until the INPA is configured***].

FDP_IFF.1(b) Simple security attributes (ONPA Interface)

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

FDP_IFF.1.1(b)

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

- ***Subject – ONPA Interface with security attributes:***
  - ***Network interface name***
  - ***Zone***
  - ***IP address***
  - ***Subnet mask***
- ***Information – Outbound traffic security attributes:***
  - ***Destination IP address***
  - ***Destination port***
  - ***Network interface name***
  - ***Protocol type (UDP, TCP)***
  - ***Protocol state (UDP, TCP states: new, established)***

]

FDP_IFF.1.2(b)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [***if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the data is allowed to flow***.].

FDP_IFF.1.3(b)

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

FDP_IFF.1.4(b)

The TSF shall explicitly authorize an information flow based on the following rules: [***no explicit authorization rules***].

FDP_IFF.1.5(b)

The TSF shall explicitly deny an information flow based on the following rules: [***no data can flow until the ONPA is configured***]].

FDP_IFF.1(c) Simple security attributes (Flow)

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

FDP_IFF.1.1(c)

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

- ***Subject – DFP with security attributes***
  - ***Service***
    - ***Service name***
    - ***Flow type (TCP or UDP)***
    - ***Directional mode (bidirectional or unidirectional)***
    - ***Data mode (message (TCP, UDP), stream (UDP))***
  - ***Filter***
    - ***Filter name***
    - ***Filter type***
    - ***Filter file name***
  - ***Flow***
    - ***Flow name***
    - ***Client IP address***
    - ***Client subnet mask***
    - ***Source network interface name***
    - ***Service port (server/listening port facing inbound)***
    - ***Service name***
    - ***Filter name***
    - ***Destination network interface name***
    - ***Destination IP address:port***

- ***Information – Data traffic with security attributes:***
  - ***Source IP address***
  - ***Destination IP address***
  - ***Destination port***
  - ***Network interface name***
  - ***Protocol type (UDP, TCP)***
  - ***Protocol state (UDP, TCP states: New, Established)***

].

FDP_IFF.1.2(c)

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [***if the configured policies allow the information flow based on a combination of subject security attributes and information security attributes, then the data is allowed to flow.***].

FDP_IFF.1.3(c)

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

FDP_IFF.1.4(c)

The TSF shall explicitly authorize an information flow based on the following rules: [***no explicit authorization rules***].

FDP_IFF.1.5(c)

The TSF shall explicitly deny an information flow based on the following rules: [***no data can flow until the service, filter, and flow are defined***].

6.2.3 Class FIA: Identification and Authentication

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 TSF-mediated actions on behalf of that user.

6.2.4 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes (INPA Interface)

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1(a)

The TSF shall enforce the [***INPA Information Flow SFP***] to restrict the ability to [query, modify, delete] the security attributes [***listed in the INPA Security Attributes column in*** Table 11] to [***the roles and operations listed in the Role and Operation columns in*** Table 11].

Table 11 – Security Attributes (INPA Interface)

Role	Operation	INPA Security Attributes
RO	Query	• Subject – **INPA** Interface with security attributes: ○ Network interface name ○ Zone ○ IP address ○ Subnet mask • Information – Inbound data with security attributes: ○ Protocol type (UDP, TCP) ○ Protocol state (UDP, TCP states: new, established)
RW	Query, Modify, Delete	

FMT_MSA.1(b) Management of security attributes (ONPA Interface)

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1(b)

The TSF shall enforce the [***ONPA Information Flow SFP***] to restrict the ability to [query, modify, delete] the security attributes [***listed in the ONPA Security Attributes column in*** Table 12] to [***the roles and operations listed in the Role and Operation columns in*** Table 12].

Table 12 – Security Attributes (ONPA **Interface)**

Role	Operation	ONPA **Security Attributes**
RO	Query	• Subject – **ONPA** Interface with security attributes: ○ Network interface name ○ Zone ○ IP address ○ Subnet mask • Information – Outbound data with security attributes: ○ Destination IP address ○ Destination port ○ Network interface name ○ Protocol type (UDP, TCP) ○ Protocol state (UDP, TCP states: new, established)
RW	Query, Modify, Delete	

FMT_MSA.1(c) Management of security attributes (Flow)

Dependencies: [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1(c)

The TSF shall enforce the [***Flow SFP***] to restrict the ability to [query, modify, delete] the security attributes [***listed in the Flow Security Attributes column in*** Table 13 ***and specified in the SFPs****]* to [***the roles and operations listed in the Role and Operation columns in*** Table 13].

Table 13 – Security Attributes (Flow**)**

Role	Operation	Flow **Security Attributes**
RO	Query	• Subject – DFP ○ Service – Service name, Flow type, Directional mode, Data mode ○ Filter – Filter name, Filter type, Filter file name ○ Flow – Flow name, Flow type, Client IP address, Client subnet mask, Source network interface name, Service port, Service name, Filter name, Destination network interface name, Destination IP address:port • Information – Data traffic between the INPA and ONPA interfaces ○ Source IP address ○ Destination IP address ○ Destination port ○ Network interface name ○ Protocol type (UDP, TCP) ○ Protocol state (UDP, TCP states: New, Established)
RW	Query, Modify, Delete	

FMT_MSA.3(a) Static attribute initialization (INPA Interface)

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

FMT_MSA.3.1(a)

The TSF shall enforce the [***INPA Information Flow SFP***] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(a)

The TSF shall allow the [***RW administrator***] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(b) Static attribute initialization (ONPA Interface)

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

FMT_MSA.3.1(b)

The TSF shall enforce the [***ONPA Information Flow SFP***] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(b)

The TSF shall allow the [***RW administrator***] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(c) Static attribute initialization (Flow)

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

FMT_MSA.3.1(c)

The TSF shall enforce the [***Flow SFP***] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(c)

The TSF shall allow the [***RW administrator***] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

- ***Assign a role to an account***
- ***Review audit records***
- ***Import Lua files***
- ***Configure the INPA and ONPA Interface security attributes***
- ***Configure the Flow security attributes***

].

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1

The TSF shall maintain the roles [***RO and RW***].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

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 CC EAL4+ augmented with ALC_FLR.2. Table 14 summarizes these requirements.

Table 14 – 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 controls
	ALC_FLR.2 Flaw reporting procedures
	ALC_LCD.1 Developer defined life-cycle processes
	ALC_TAT.1 Well-defined development tools
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 Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 15 lists the security functionality and their associated SFRs.

Table 15 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_IFC.1(a)	Subset information flow control (INPA Interface)
	FDP_IFC.1(b)	Subset information flow control (ONPA Interface)
	FDP_IFC.1(c)	Subset information flow control (Flow)
	FDP_IFF.1(a)	Simple security attributes (INPA Interface)
	FDP_IFF.1(b)	Simple security attributes (ONPA Interface)
	FDP_IFF.1(c)	Simple security attributes (Flow)
Identification and Authentication	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1(a)	Management of security attributes (INPA Interface)
	FMT_MSA.1(b)	Management of security attributes (ONPA Interface)
	FMT_MSA.1(c)	Management of security attributes (Flow)
	FMT_MSA.3(a)	Static attribute initialisation (INPA Interface)
	FMT_MSA.3(b)	Static attribute initialisation (ONPA Interface)
	FMT_MSA.3(c)	Static attribute initialisation (Flow)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles

7.1.1 Security Audit

The TOE generates audit records for the startup and shutdown of the TOE components. The startup and shutdown of the TOE components results in the startup and shutdown of the audit functionality. The TOE also generates audit records for configuration changes, commands entered from the CLI, and flow events. Log files include a unique identifier for each EDG server. TOE-generated audit events are written to the `xguard-admin.log` and `xguard-flow.log` files. From the TOE's CLI, administrators may view the following log files: audit.log, xguard-admin.log and xguard-flow.log. These log files are automatically rotated to prevent disk space issues that could lead to the TOE shutting down.

- The `xguard-admin.log` file contains audit records for events generated by successful commands entered by administrators from the CLI, and configuration events generated by administrator activity in the DFM module.
- The `xguard-flow.log` file includes startup and shutdown of the audit function events, NPA events and information about the type of flow and flow metrics.

An administrator can view the log files from the CLI by issuing the **`log view`** command, followed by either the **`admin`** or **`flow`** keyword. For example, to view the `xguard-admin.log` file, a RW administrator enters the **`log view admin`** command and uses optional parameters to view logs in their entirety or to filter what is displayed.

The audit startup and shutdown is logged in the `xguard-flow.log` file. The startup and shutdown of the TOE coincides with the startup and shutdown of the audit function. When the TOE starts up an audit record is generated with event ID 9000, `evt=9000`, and the message "`msg=Starting Forcepoint Data Guard`". When the TOE shuts down an audit event is generated with event ID9001, `evt=9001`, and the message "`msg=Stopping Forcepoint Data Guard`". These records can be viewed from the **FDG CLI** TSFI by a RW administrator using the **`log view flow display find evt=9000`** or **`log view flow display find evt=9001`** commands.

The TOE environment provides reliable timestamps for the audit records.

Table 16 describes the fields and token name arguments contained in both the `xguard-admin.log` and `xguard-flow.log` files, except for the `Component*` field, which is **not** in the `xguard-admin.log` file. Any combination of token name command arguments can be in both files.

Table 16 – Admin and Flow Log Files

Field Name	Description
Severity	This field identifies the severity of the event.
Timestamp	This field identifies the timestamp in MM DD HH:MM:SS Linux UTC format.
Hostname	This field identifies the hostname.
Component*	This field identifies the component, which can have the following values: `xg-in-npa-tcp, xg-out-npa-tcp, xg-in-npa-tcp-udp, xg-out-npa-udp`
Token=Value pairs	This contains the command arguments or flow information.
Token Name Argument	**Description**
`evt`	This argument provides the Event ID.
`user`	This argument provides the user name.
`uid`	This argument identifies the user id.
`flow`	This argument provides the flow name.
`dir`	This argument provides the flow direction, either "fwd" or "rev".
`id`	This argument provides the connection id or file id.
`action`	This argument provides the action.
`status`	This argument provides the status.
`server`	This argument provides the server name.
`cmd`	This argument provides the command name.
`src`	This argument provides the source IP that an event refers to.
`dst`	This argument provides the destination IP that an event refers to.
`spt`	This argument provides the source port.
`dpt`	This argument provides the destination port.
`errno`	This argument provides the errno number from the sys call.
`sterror`	This argument provides the message describing the errno.
`func`	This argument provides the sys call name.
`caller`	This argument provides the caller of sys call.
`fmsg`	This argument provides the user message.
`msg`	This argument provides the detail message (last one).

Field Name	Description
`name`	This argument provides the file name.

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

7.1.2 User Data Protection

The TOE is installed in a secure DENY ALL configuration. The INPA and ONPA interfaces must be configured before receiving any data and no data is allowed to flow until the DFP's interface, service, filter, and flow security attributes are defined. Data is inspected at the TOE boundary by the **INPA** for a matching IP address and subnet mask to determine if traffic is passed or dropped. If the traffic is passed, then the data is buffered and is read by the DFP. The **DFP** reads the buffered inbound data and applies filtering logic to determine if data is passed to the **ONPA**, or is dropped. The **DFP** filtering decisions are based on a service definition, Lua filter rules, and flow attributes. A service definition includes the following: service name, flow type (TCP or UDP), directional mode (unidirectional or bidirectional), and data mode (stream or message). The service definition determines what filtering rules are applied by the **DFP** and include the following attributes: assigned filter name, filter type, and filter file name. The **ONPA** receives its data payload from the **DFP** if the IP address and subnet mask security attributes match, otherwise it is dropped. If allowed to pass the **ONPA** sends the DFP-filtered data to an external destination endpoint. If the bidirectional mode is defined, then responses to originating requests are sent from the ONPA to the DFP. The **DFP** filters the reverse data. There are default rules for matching related and established flows that allow for reverse traffic to flow without needing explicit rules. If the Lua rule file does not have the reverse data flow defined within it, then no reverse data is allowed.

The global configuration file and any affected individual configuration files for **INPA**, **ONPA**, and **DFP** are updated after a RW administrator makes changes from the CLI. The changes take effect after a restart. A RW administrator can enter the **`flow restart`** command or a restart can be initiated by **DFM**. Please see section 6.2.2 for the complete list of **INPA**, **ONPA**, and **Flow** security attributes.

A RW administrator creates Lua files and imports them to the TOE using the **`import_files`** command from the CLI. When a flow enters an interface, it is buffered and passed to the **DFP**. The **DFP** uses its internal XG filter functions to interact with the Lua filters. The **DFP** processes the buffered data against the filtering rules in the named Lua file. If the buffered data is allowed, the data flows between the NPA interfaces, otherwise the data is dropped from the flow.

There are default rules for matching related and established flows that allow for reverse traffic to flow without needing explicit rules. The **DFP** filters the reverse data. If the Lua rule file does not have the reverse data flow defined within it, then no reverse data is allowed.

TOE Security Functional Requirements Satisfied: FDP_IFC.1(a), FDP_IFC.1(b), FDP_IFC.1(c), FDP_IFF.1(a), FDP_IFF.1(b), FDP_IFF.1(c).

7.1.3 Identification and Authentication

No TSF functionality is available to an administrator until the administrator is identified by the TOE. The administrator enters their credentials at the **FDG CLI**. After the administrator's credentials are verified, the TOE identifies the administrator by associating the administrator's username with the username of the logged in account. The administrator assumes the account's assigned role and the role's privileges and access to the TOE.

TOE Security Functional Requirements Satisfied: FIA_UID.2.

7.1.4 Security Management

Administrators configure and manage the TOE's security functionality from the **FDG CLI**, which they connect to using either a remote SSH connection or a local console connection. The administrator is assigned the role associated with the logged in account and the TOE grants privileges associated with the account. There are only two TOE roles: read-write (RW) and read-only (RO). The RW role (assigned to a RW administrator) provides complete administrative access to configure and manage the TOE. The RO role (assigned to a RO administrator) provides read-only access and includes limited privileges to view configuration data.

The **FDG CLI** has four modes and each mode has a set of commands for configuration and management of the TOE. The role assigned to an administrator determines which mode or modes can be accessed.

- Standard Mode is a read-only mode that is limited to read-only commands.
- Privileged Mode is a mode that provides all available commands.
- Configuration Mode is a mode that provides only configuration commands.
- Configuration Build Mode is a mode that provides only the configuration commands relevant to the feature being configured or managed.

All administrators can access the Standard Mode but only RW administrators can access the other modes.

Only RW administrators can manage the TOE's security functionality, performing the following management tasks:

- Assign a role to an account using **`user add <user name> <RO|RW>`**
- Import Lua files using **`import_files <path to Lua file>`**
- Configure the INPA, ONPA, and Flow security attributes using the commands from Chapter 6.2 "Configuring a TCP/UDP Data Flow" in the TOE Admin Guide.

Only RW administrators can perform the following:

- Review audit records using **`log view`** <**`admin`** | **`flow`**>

See section 6.2.4 for the INPA, ONPA, and Flow security attributes that are configured by a RW administrator.

The TOE is installed with the default Admin account. New accounts are added with the default account and associated with either the RO or RW role.

A RW administrator uses the **FDG CLI** to configure the security attributes and the data flows. To allow a flow, a RW administrator must import a Lua file, configure the INPA and ONPA interfaces, and configure the **Flow** security attributes listed under the Service, Filter, and Flow bullet points above.

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

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version CC:2022, Release 1.

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. The tables in this section 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 and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 17 provides a mapping of the objectives to the threats they counter.

Table 17 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.FLOW An attacker may try to gain access to the destination network or to data in transit to the destination network by bypassing the data flow policies placed on the networks.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE's flow policies are recorded.
	O.FLOW The TOE must ensure that data will flow only as defined in the Information Flow SFPs.	O.FLOW ensures that data flows only as defined by the Information Flow SFPs, which is only configurable by a RW administrator and cannot be bypassed.
T.REVERSE_FLOW An attacker may try to gain access to the data that is sent in reply from the destination network by bypassing the data flow policies placed on the networks.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE's flow policies are recorded.
	O.FLOW The TOE must ensure that data will flow only as defined in the Information Flow SFPs.	O.FLOW ensures that data flows only as defined by the Information Flow SFPs, which is only configurable by a RW administrator and cannot be bypassed.
T.UNDETECTED_ACTIONS An attacker may take actions that adversely affect the security of the TOE assets and these actions remain undetected so that their effects cannot be effectively countered.	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that security relevant events for all configuration changes made to the TOE and data flow events performed by the TOE are recorded.

Threats	Objectives	Rationale
T.UNPRIVILEGED An underprivileged user may try to change the TOE configuration and compromise its security functions.	O.ACCESS The TOE must enforce an access control policy to provide appropriate access to administrators that view or manage TOE resources based on their assigned roles.	O.ACCESS ensures that an attacker cannot access the TOE, which can only be accessed by an identified administrator with an assigned role. The administrator's role determines what command line functionality is available to the administrator.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data.	O.ADMIN ensures that the TOE provides the management functionality necessary to manage TOE functions and data.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.IDENTIFY The TOE must be able to identify administrators prior to allowing access to TOE administrative functions and data.	O.IDENTIFY ensures that all administrators that attempt to access the TOE are identified as administrators with permission to use the TOE before they can perform any actions.

Every threat is mapped to one or more objectives, demonstrating that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Assumptions

Table 18 gives a mapping of assumptions and the environmental objectives that uphold them.

Table 18 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.PLATFORM The TOE is installed on the appropriate, dedicated hardware and the platform contains only the approved applications needed to support the TOE as per the installation guidance.	OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. The hardware and RHEL OS with SELinux and Iptables modules are installed according to the guidance to provide the functionality necessary to support the secure operation of the TOE.	OE.PLATFORM ensures that the administrator-installed hardware and RHEL OS with SELinux and Iptables modules provide the functionality necessary to support the TOE.
	NOE.ADMIN Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.	The TOE is installed on the appropriate, dedicated hardware and the platform contains only the approved software required to support the TOE.
A.NETCON The TOE environment provides network connectivity between the TOE and external networks.	OE.NETWORK The TOE environment must be implemented such that the TOE is logically connected to only the defined external inbound and outbound networks and to no other networks.	OE.NETWORK satisfies the assumption that the TOE will be deployed with the appropriate network connections.
A.TIMESTAMP The IT environment provides the TOE with the necessary and reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.
A.PHYSICAL The TOE is located within a controlled access facility.	OE.PROTECT The TOE environment must protect itself and the TOE from external access attempts or attempts to intercept the data transiting the TOE. The TOE environment must provide logical and physical security controls to protect the network resources and data at the level appropriate to the sensitivity of the data.	OE.PROTECT satisfies the assumption that physical security is provided within the TOE environment to provide appropriate protection to the network resources.

Assumptions	Objectives	Rationale
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external access attempts or attempts to intercept the data transiting the TOE. The TOE environment must provide logical and physical security controls to protect the network resources and data at the level appropriate to the sensitivity of the data.	OE.PROTECT satisfies the assumption that the TOE environment provides security controls, which protect the TOE software from external interference or tampering.
A.ADMIN There are one or more competent individuals assigned to manage the TOE and the security of the information it contains. Administrators are trusted and assumed not to be willfully hostile to the TOE.	NOE.ADMIN Sites deploying the TOE will provide competent, non-hostile administrators who are appropriately trained and follow all administrator guidance. Administrators will ensure the system is used securely.	NOE.ADMIN satisfies the assumption that the TOE administrators are non-hostile, appropriately trained and follow all guidance.
A.AUTHENTICATION The platform that the TOE is installed on will provide adequate authentication methods for TOE administrators.	OE.AUTHENTICATE The TOE environment must provide user authentication.	OE.AUTHENTICATE satisfies the assumption that TOE administrators are authenticated by the OS.

Every assumption is mapped to one or more objectives, demonstrating that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

There are no extended security functional requirements defined for this TOE.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE security 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 19 shows a mapping of the objectives and the SFRs that support them.

Table 19 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must enforce an access control policy to provide appropriate access to administrators that view or manage TOE resources based on their assigned roles.	FAU_SAR.1 Audit review	The requirement supports the O.ACCESS objective by ensuring that only authorized administrators with the RW role can view the audit data.
	FMT_MSA.1(a) Management of security attributes (INPA Interface)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.

Objective	Requirements Addressing the Objective	Rationale
	FMT_MSA.1(b) Management of security attributes (ONPA Interface)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.
	FMT_MSA.1(c) Management of security attributes (Flow)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.
	FMT_MSA.3(a) Static attribute initialisation (INPA Interface)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.
	FMT_MSA.3(b) Static attribute initialisation (ONPA Interface)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.
	FMT_MSA.3(c) Static attribute initialisation (Flow)	The requirement meets the O.ACCESS objective by ensuring that only the identified administrators are allowed role-based access to the administrative functions to manage the security behavior of the TOE.
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data.	FMT_MSA.1(a) Management of security attributes (INPA Interface)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides the functionality required to manage the TOE security attributes.
	FMT_MSA.1(b) Management of security attributes (ONPA Interface)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides the functionality required to manage the TOE security attributes.
	FMT_MSA.1(c) Management of security attributes (Flow)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides the functionality required to manage the TOE security attributes.
	FMT_MSA.3(a) Static attribute initialisation (INPA Interface)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3(b) Static attribute initialisation (ONPA Interface)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_MSA.3(c) Static attribute initialisation (Flow)	The requirement meets the O.ADMIN objective by ensuring that the TOE provides restrictive default values for security attributes and specifies alternative initial values to override the default values when an object or information is created.
	FMT_SMF.1 Specification of management functions	The requirement meets the O.ADMIN objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the O.ADMIN objective by ensuring that the TOE associates administrators with roles to provide access to TSF management functions and data.

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies and provide the authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement supports the O.AUDIT objective by ensuring that the TOE generates security related events, including relevant details about the event which provide information for the management of the TSF.
	FAU_SAR.1 Audit review	The requirement meets the O.AUDIT objective by ensuring that the TOE provides the ability to review logs.
O.FLOW The TOE must ensure that data will flow only as defined in the Information Flow SFPs.	FDP_IFC.1(a) Subset information flow control (INPA Interface)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces information flow control on the INPA and ONPA interfaces based on the implemented policy.
	FDP_IFC.1(b) Subset information flow control (ONPA Interface)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces information flow control on the INPA and ONPA interfaces based on the implemented policy.
	FDP_IFC.1(c) Subset information flow control (Flow)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces information flow control on the DFP based on the implemented policy.
	FDP_IFF.1(a) Simple security attributes (INPA Interface)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces the information flow control SFP on the INPA and ONPA interfaces based on the security attributes.
	FDP_IFF.1(b) Simple security attributes (ONPA Interface)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces the information flow control SFP on the INPA and ONPA interfaces based on the security attributes.
	FDP_IFF.1(c) Simple security attributes (Flow)	The requirement meets the O.FLOW objective by ensuring that the TOE enforces the information flow control SFP on the DFP based on the security attributes.
O.IDENTIFY The TOE must be able to identify administrators prior to allowing access to TOE administrative functions and data.	FIA_UID.2 User identification before any action	The requirement supports the O.IDENTIFY objective by ensuring that an administrator is successfully identified before allowing any other TOE-mediated actions.

8.5.2 Security Assurance Requirements Rationale

EAL4+ was chosen because it is best suited to address the stated security objectives. EAL4+ challenges vendors to use best (rather than average) commercial practices. EAL4+ allows the vendor to evaluate their product at a detailed level while benefitting from the Common Criteria Recognition Agreement, which would recognize the TOE as an EAL2+ evaluation. The chosen assurance level is appropriate for the threats defined in the environment. At EAL4+, penetration testing is performed by the evaluator assuming an attack potential of Enhanced-Basic.

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 20 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 20 – Functional Requirements Dependencies

SFR	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not included, timestamps are provided by the operating environment and this satisfies the dependency requirement.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_IFC.1(a)	FDP_IFF.1(a)	✓	
FDP_IFC.1(b)	FDP_IFF.1(b)	✓	
FDP_IFC.1(c)	FDP_IFF.1(c)	✓	
FDP_IFF.1(a)	FDP_IFC.1(a)	✓	
	FMT_MSA.3(a)	✓	
FDP_IFF.1(b)	FDP_IFC.1(b)	✓	
	FMT_MSA.3(b)	✓	
FDP_IFF.1(c)	FDP_IFC.1(c)	✓	
	FMT_MSA.3(c)	✓	
FIA_UID.2	No dependencies		
FMT_MSA.1(a)	FDP_IFC.1(a)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FDP_IFC.1(b)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(c)	FDP_IFC.1(c)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(a)	FMT_MSA.1(a)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(b)	FMT_MSA.1(b)	✓	
	FMT_SMR.1	✓	
FMT_MSA.3(c)	FMT_MSA.1(c)	✓	
	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.

9. Acronyms and Terms

Table 21 defines the acronyms and terms used throughout this document.

Table 21 – Acronyms and Terms

Acronym	Definition
AMI	Amazon Machine Image
EDG	Everfox Data Guard
API	Application Programming Interface
CC	Common Criteria
CD	Compact Disk
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
DFM	Data Flow Manager
DFP	Data Filtering Process
EAL	Evaluation Assurance Level
EC2	Elastic Compute Cloud
EULA	End User License Agreement
FDG	Forcepoint Data Guard
GB	Giga Byte
ID	Identification
INPA	Inbound Network Protocol Adapter
IP	Internet Protocol
ISO	Optical Disc Image
IT	Information Technology
JSON	JavaScript Object Notion
NPA	Network Protocol Adapter
ONPA	Outbound Network Protocol Adapter
OS	Operating System
OSP	Organizational Security Policy
PDF	Portable Document Format
PKI	Public Key Infrastructure
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
RO	Read-only
RW	Read-write
SAR	Security Assurance Requirement
SELinux	Security Enhanced Linux
SFR	Security Functional Requirement
SFP	Security Function Policy

Acronym	Definition
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
TSS	TOE Security Specification
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
XML	Extensible Markup Language

Prepared by:

Corsec Security, Inc.

12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22033
United States of America

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