Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 2/20

(Certification No.)

Prodotto: Forcepoint Data Guard v3.0

(Product)

Sviluppato da: Forcepoint LLC

(Developed by)

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.2)

Il Direttore
(Dott.ssa Eva Spina)

[ORIGINAL DIGITALLY SIGNED]

Roma, 26 maggio 2020

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Forcepoint Data Guard v3.0

OCSI/CERT/CCL/05/2019/RC

Version 1.0

26 May 2020

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	26/05/2020

2 Table of contents

3 Acronyms

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CD-ROM	Compact Disc - Read-Only Memory
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DFM	Data Flow Manager
DFP	Data Filtering Process
DPCM	Decreto del Presidente del Consiglio dei Ministri
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GB	Gigabyte
HTTPS	HyperText Transfer Protocol over Secure Socket Layer
INPA	Inbound Network Protocol Adaptor
IP	Internet Protocol
IT	Information Technology
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
NPA	Network Protocol Adapter
OCSI	Organismo di Certificazione della Sicurezza Informatica
ONPA	Outbound Network Protocol Adaptor
OS	Operating System
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
RO	Read-Only

RW	Read-Write
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface
UDP	User Datagram Protocol

4 References

4.1 Criteria and regulations

[CC1] CCMB-2012-09-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2012-09-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2012-09-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2012-09-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[GADM] “Forcepoint Data Guard Administrator’s Guide”, Version 3.0.0.0-9005, 28 February 2019

[GCCS] “Forcepoint Data Guard Guidance Documentation Supplement”, Version 0.2, 6 November 2019

[ETR] “Forcepoint Data Guard v3.0” Evaluation Technical Report, v1, CCLab Software Laboratory, 14 April 2020

[ST] “Forcepoint LLC Forcepoint Data Guard v3.0 Security Target”, Version 0.8, Corsec Security, Inc., 16 March 2020

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on https://www.sogis.eu/.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL4.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on https://www.commoncriteriaportal.org/.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “Forcepoint Data Guard v3.0”, developed by Forcepoint LLC, hereinafter also referred to as “Forcepoint Data Guard” or “FDG”.

The TOE 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.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [ST]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_FLR.2, according to the information provided in the Security Target [ST] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However, the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product “Forcepoint Data Guard v3.0” to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [ST], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	Forcepoint Data Guard v3.0.0.0 Build Number 9005
Security Target	“Forcepoint LLC Forcepoint Data Guard v3.0 Security Target”, Version 0.8 [ST]
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.2
Developer	Forcepoint LLC
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	7 October 2019
Evaluation ending date	15 April 2020

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [ST] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of the TOE. For a detailed description, please refer to the Security Target [ST].

The TOE “Forcepoint Data Guard v3.0” (FDG) is a software-only product designed to inspect, validate, and filter network traffic using a flexible Lua-based rules engine that allows administrators to implement data protection and sharing policies for enterprise data.

The TOE runs on commercially available server hardware and is deployed between domains or networks of different security or classification levels. The TOE includes only the FDG software application. The TOE inspects and filters transiting data flows by

applying the filtering rules to the traffic that flows between the NPAs. By default, no data can flow between the NPAs unless the rules allow the flow.

Administrators implement rules to define unidirectional or bidirectional flow. The filtering rules to allow or drop a data payload can be applied from a high-level (interface, network zone, or protocol) down to the byte level for deep content inspection.

For a detailed description of the TOE, consult sect. 1.3, 1.4, 1.5 and 1.6 of the Security Target [ST]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

The TOE is separated into the following components:

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

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.

The DFP provides the core filtering capabilities for the TOE. The DFP handles the input/output operations for the flow data and hosts the Lua-based Filtering Engine. Administrators implement rule sets 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 INPA receives traffic 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 sending any of the allowed data to the DFP for filtering.

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.

Figure 1 illustrates the physical scope and the physical boundary of the TOE.

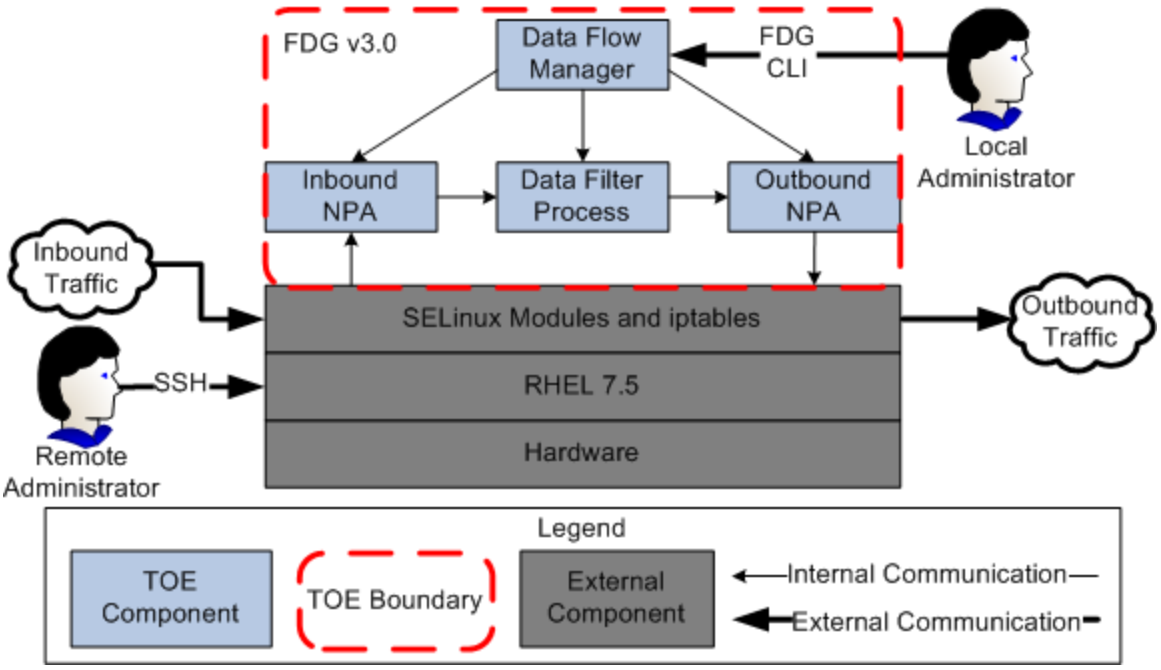

Figure 1 - Physical TOE boundary

The TOE runs on the RHEL 7.5 OS. RHEL provides core services such as authentication, data storage, SSH for remote authentication, and TCP/IP networking support.

Management of the TOE is performed using either a remote SSH connection or the local RHEL console to access the CLI of the TOE.

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [ST].

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [ST]. The most significant aspects are summarized below:

- **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. Administrators may view logs from the TOE's CLI.
- **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.
- **Identification and Authentication**: the TOE requires administrators be identified by their TOE roles before gaining access to any TOE data or functionality.
- **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 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.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [ST].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [ST] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

Please refer to the Security Target [ST] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [ST]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 15 April 2020 with the issuance by LVS of the Evaluation Technical Report [ETR], which was approved by the Certification Body on 27 April 2020. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "Forcepoint Data Guard v3.0" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.2, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_FLR.2.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass

Assurance classes and components		Verdict
Identification of security measures	ALC_DVS.1	Pass
Flaw reporting procedures	*ALC_FLR.2*	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 - Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product “Forcepoint Data Guard v3.0” are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all the assumptions described in sect. 3.3 of the Security Target [ST] are respected.

This Certification Report is valid for the TOE in its evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([GADM], [GCCS]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

The TOE is distributed to customers in two ways: on CD-ROM (physical distribution) or as a download (digital distribution).

All physical media shipments are packaged and shipped via international delivery services. The Forcepoint Product Distribution Team tracks the package to ensure delivery acceptance. The Installation CD, and the Documentation CD are placed into vinyl media sleeves, along with a copy of the Forcepoint Software License Agreement, product cover letter, and the Forcepoint Software Maintenance Agreement. These items are contained within the Installation Media Packet, which is sealed with a tamper evident label. The Installation Media Packet is inserted into a padded Manila envelope, which is inserted into a delivery company package for shipment.

Upon receipt of the package, an administrator verifies the integrity of the Installation CD (*fdg_3-0-0-0-9005_GA_2019-02-28*) and the Documentation CD (*fdg_3-0-0-0-9005_Documentation_2019-02-28*) by computing and checking their SHA-256 checksums.

For orders that require digital distribution, the TOE is distributed in ISO disk image format. All digital downloads are provided using Kiteworks links. Folders with the needed files are created on Kiteworks that are restricted to the Product Distribution Team and the customer that will download them. The Kiteworks links are temporary with a maximum of one week before they become invalid. The customer downloads the software over an HTTPS connection using the link to Kiteworks.

After downloading the ISO files, the administrator verifies the integrity of the Installation image file (*fdg_3-0-0-0-9005_GA_2019-02-28.iso*) and the Documentation image file (*fdg_3-0-0-0-9005_Documentation_2019-02-28.iso*) by computing and checking their SHA-256 checksums.

Verification of checksums values requires that the customer contact Forcepoint.

9.2 Identification of the TOE

After installation, the actual version of the TOE can be verified by issuing the “show version” command at the FDG CLI. The command must return the following string:

```
Forcepoint Data Guard 3.0.0.0-9005
```

9.3 Installation, initialization and secure usage of the TOE

TOE installation and configuration should be done following the instructions in the appropriate sections of the guidance documentation provided with the product to the customer.

The following documents contain information for the secure initialization of the TOE and the preparation of its operational environment in accordance with the security objectives specified in the Security Target [ST]:

- “Forcepoint Data Guard Administrator’s Guide”, Version 3.0.0.0-9005, 28 February 2019 [GADM]
- “Forcepoint Data Guard Guidance Documentation Supplement”, Version 0.2, 6 November 2019 [GCCS]

10 Annex B – Evaluated configuration

The TOE is the software-only product “Forcepoint Data Guard v3.0”, developed by Forcepoint LLC.

The TOE is identified in the Security Target [ST] as “Forcepoint Data Guard v3.0.0.0 Build Number 9005”. The name, version number, and build number uniquely identify the TOE.

The TOE has only one evaluated configuration, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

For more details, please refer to sect. 1.4 of the Security Target [ST].

10.1 TOE operational environment

In Table 2 are summarized the components of the operational environment of the TOE to allow its correct working. Inbound and outbound networks are required for the TOE to filter traffic.

For more details, please refer to sect. 1.5 of the Security Target [ST].

Component	Requirement
Operating System	Red Hat Enterprise Linux (RHEL) 7.5 including the following: • SELinux • Iptables • OpenSSH Server
Hardware	The minimum hardware requirements include the following: • At least one network interface card • A CD drive • 2 GB of memory • 40 GB of storage See the minimum hardware requirements for RHEL 7 version 5 listed at https://access.redhat.com/articles/rhel-limits.

Table 2 - TOE operational environment components

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities. For the assurance level EAL4, augmented with ALC_FLR.2, such activities include the following three steps:

- evaluation of the tests performed by the Developer in terms of coverage and level of detail;
- execution of independent functional tests by the Evaluators;
- execution of penetration tests by the Evaluators.

11.1 Test configuration

All testing activities have been carried out at the LVS premises.

For the execution of the tests, the Developer has made available to the LVS a set of resources equivalent to those used to carry out its tests.

The Evaluators created the test environment compliant to the description in the Developer's test documentation. In addition to the equipment described in the Security Target [ST] for the TOE environment, the test environment required two additional Linux hosts used to send traffic through the TOE.

The Evaluators installed and configured the TOE in the test environment following the preparative procedures described in the operative documentation listed in sect. 9.3. After configuration of the TOE the Evaluators verified that the TOE was installed properly and in a known state.

11.2 Functional tests performed by the developer

11.2.1 Testing approach

The Developer's test approach is to perform functional tests to demonstrate that the TSF and TSFI perform as specified in the Security Target [ST] and in the functional specification, TOE design and security architecture description.

The Developer created test cases that test more functionalities of the TOE at a time, instead of creating fewer test cases for every functionality separately. Hence the number of the Developer's test cases is reduced, but the tests are comprehensive.

11.2.2 Test coverage

The Evaluators have examined the test plan presented by the Developer and verified the complete coverage of the functional requirements SFR and the TSFIs described in the functional specification.

11.2.3 Test results

The Evaluators executed all the test cases described in the test plan presented by the Developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the Evaluators

Therefore, the Evaluators have designed independent testing to verify the correctness of the TSFI.

The Evaluators did not require any special testing tools to check the TSFI selected for independent testing.

In the design of independent tests, the Evaluators have considered aspects that in the Developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The Evaluators also designed and executed some tests independently from similar tests of the Developer, based only on the evaluation documentation.

All independent tests performed by Evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The Evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the Security Target [ST], sect. 1.2.

In a first phase, the Evaluators have conducted researches using various sources in the public domain, in order to identify known vulnerabilities applicable to the TOE. They identified one potential vulnerability in the Data Filtering Process (DFP), a customized version of the Lua runtime environment embedded in the TOE's software.

In a second step, the Evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture, operational documentation) to identify any additional potential vulnerabilities of the TOE.

From these analyses, the Evaluators have actually determined the presence of three potential vulnerabilities:

1. missing patch for CVE-2014-5461;

2. the backup and export-files FDG CLI commands could provide information about the internal state and configuration of the TOE;

3. the restore and import-files FDG CLI commands could result in external modification of the TOE configuration data, hence resulting in unauthorized access and privilege escalation.

Although, the FDG backup and restoration functionalities are not part of the TOE, vulnerabilities 2 and 3 can potentially be exploited to mount further attacks to the TSF.

The Evaluators analysed in detail the potential vulnerabilities identified in the previous steps, and devised several attack scenarios and penetration tests to verify their actual exploitability in the TOE's operational environment, considering an Enhanced-Basic attack potential.

At the end of all the penetration testing sessions, the Evaluators could conclude that no attack scenario with potential Enhanced-Basic or lower can be completed successfully in the operational environment of the TOE as a whole, and all the identified vulnerabilities are considered residual, i.e., they can be exploited only by an attacker with attack potential beyond Enhanced-Basic.

In particular, vulnerability 1 requires a Moderate attack potential and resulted not fully exploitable, while the other two require a High attack potential to be effectively exploited.