secunet(wall

# Security Target

## secunet(wall 6.0.1

Certification-ID: BSI-DSZ-CC-1116

Document Version: 1.8

Document Date: 12/12/2019

secunet
secunet Security Networks AG

**Documentation history**

| Version | Date | Change(s) | Author(s) |
|---|---|---|---|
| 0. 1 | xx/06/2018 | Initial Draft | Peter Jung (SRC) |
| 0.2 | 16/10/2018 | Second Draft (for internal QA) | Peter Jung (SRC) |
| 0.3 | 24/10/2018 | Third Draft | Peter Jung (SRC) |
| 0.9 | 28/11/2018 | added security architecture overview necessary for ASE_TSS.2 | Peter Jung (SRC) |
| 1.0 | 28/11/2018 | Review secunet | Secunet |
| 1.1 | 18/03/2019 | ST update after BSI kickoff meeting | Peter Jung (SRC) |
| 1.2 | 07/05/2019 | ST update after ITSEF comments | Peter Jung (SRC) |
| 1.3 | 05/06/2019 | ST update after ITSEF comments | Secunet |
| 1.4 | 12/06/2019 | ST update after ITSEF comments | Secunet |
| 1.5 | 12/08/2019 | ST update after ITSEF comments | Secunet |
| 1.6 | 06/12/2019 | ST update after ITSEF comments | Secunet |
| 1.7 | 09/12/2019 | ST update after ITSEF comments | Secunet |
| 1.8 | 12/12/2019 | ST update after ITSEF comments | Secunet |

# Contents

Contents ..... 3

List of Tables ..... 6

1 ST INTRODUCTION ..... 7

1.1 ST reference and TOE reference ..... 7

1.2 TOE Overview ..... 7

1.2.1 Usage, major security features and TOE type ..... 7
1.2.2 Required non TOE hardware/software/firmware ..... 10

1.3 TOE Description ..... 11

1.3.1 Physical scope of the TOE ..... 11
1.3.2 Logical scope of the TOE ..... 11
1.3.2.1 Information Flow Protection ..... 12
1.3.2.2 Identification and Authentication ..... 12
1.3.2.3 Management ..... 12
1.3.2.4 Container Authentication ..... 12
1.3.2.5 Audit Data ..... 13
1.3.2.6 Components ..... 13

2 CONFORMANCE CLAIM ..... 14

2.1 CC Conformance Claim ..... 14

2.2 PP and security requirement package claim ..... 14

2.3 CC Conformance Claim Rationale ..... 14

2.4 Package Claim ..... 14

3 SECURITY PROBLEM DEFINITION ..... 15

3.1 Assets ..... 15

3.2 Subjects ..... 16

3.3 Assumptions ..... 17

3.4 Threats ..... 18

3.5 Organisational security policies ..... 18

4 STATEMENT OF SECURITY OBJECTIVES ..... 19

4.1 Security Objectives for the TOE ..... 19

4.2 Security Objectives for the Operational Environment ..... 20

4.3 Security Objectives Rationale ..... 21

4.3.1 Countering the threats ....22
4.3.2 Covering the OSPs ....22
4.3.3 Covering the assumptions ....22

5 STATEMENT OF SECURITY REQUIREMENTS ....24

5.1 Security functional requirements for the TOE ....24
5.1.1 Security Audit ....26
5.1.1.1 FAU_GEN.1 Audit data generation ....26
5.1.2 Cryptographic Support (FCS) ....26
5.1.2.1 FCS_COP.1/SHA Cryptographic operation ....26
5.1.2.2 FCS_COP.1/RSA-verify Cryptographic operation ....27
5.1.2.3 FDP_IFC.1 Subset information flow control ....27
5.1.2.4 FDP_IFF.1 Simple security attributes ....28
5.1.2.5 FDP_ITC.2 Import of user data with security attributes ....29
5.1.3 User identification (UID) ....30
5.1.3.1 FIA_AFL.1 Authentication failure handling ....30
5.1.3.2 FIA_UAU.1 Timing of authentication ....30
5.1.3.3 FIA_UID.1 Timing of identification ....30
5.1.3.4 Security management (FMT) ....31
5.1.3.5 FMT_MSA.1 Management of security attributes ....31
5.1.3.6 FMT_MSA.3 Static attribute initialization ....31
5.1.3.7 FMT_SMF.1 Specification of management functions ....32
5.1.3.8 FMT_SMR.1 Security roles ....32
5.1.4 Protection of the TSF (FPT) ....32
5.1.4.1 FPT_STM.1 Reliable time stamps ....32
5.1.4.2 FPT_TDC.1 Inter-TSF basic TSF data consistency ....32

5.2 Extended Components definition ....33

5.3 Security assurance requirements for the TOE ....34

5.4 Security Requirements Rationale ....35
5.4.1 TOE functional requirements rationale ....35
5.4.2 Fulfilling the SFR dependencies ....36
5.4.3 Security assurance requirements rationale ....38

6 TOE SUMMARY SPECIFICATION ....39

6.1 TOE security functionality ....39
6.1.1 SF1 Information Flow Protection ....39
6.1.2 SF2 Management ....40
6.1.3 SF3 Container Authentication ....40
6.1.4 SF4 Security Audit ....41

6.2 Mapping between Security Functionality (SF) and Security Functional Requirements (SFRs) ....42

6.3 Self-Protection against Interference and Logical Tampering ....42

6.4 Self-Protection against Bypass ....43

7 GLOSSARY AND ACRONYMS ....44

8 REFERENCES .....45

# List of Tables

Table 1: Scope of TOE delivery ..... 11
Table 2: secunet(wall Packet Filter components ..... 13
Table 3: Assets ..... 15
Table 4: TOE Subjects ..... 16
Table 5: Assumptions ..... 18
Table 6: Threats ..... 18
Table 7: Security Objectives for the TOE ..... 19
Table 8: Security Objectives for the environment of the TOE ..... 20
Table 9: Security Objective Rationale ..... 21
Table 10: Security Functional Requirements for the TOE ..... 25
Table 11: Chosen Evaluation Assurance Requirements ..... 34
Table 12: Coverage of Security Objective for the TOE by SFRs ..... 35
Table 13: Fulfilling the SFR dependencies ..... 38

# List of Figures

Figure 1 TOE environment ..... 8
Figure 2 Toe Scope ..... 12

# 1 ST INTRODUCTION

## 1.1 ST reference and TOE reference

| | |
|---|---|
| Title: | secunet(wall Security Target |
| Sponsor: | secunet Security Networks AG |
| Editor(s): | Peter Jung (SRC) |
| Version Number: | 1.8 |
| Date: | 12/12/2019 |
| CC Version: | Version 3.1, Revision 5 |
| Assurance Level: | EAL4+, that is EAL4 augmented by ALC_FLR.2, AVA_VAN.5 and ASE_TSS.2 |
| Certification-ID: | BSI-DSZ-CC-1116 |
| Keywords: | Firewall, Packet Filter, Network Security, Information flow control |
| TOE name: | secunet(wall |
| TOE version: | Version 6.0.1 |

## 1.2 TOE Overview

### 1.2.1 Usage, major security features and TOE type

This Security Target defines the security objectives and requirements for the secunet(wall (TOE), a software product of secunet Security Networks AG.

When IP networks with different levels of security are interconnected, this is usually done by introducing special network components at the border of the networks. These components provide firewall functionality and separate the two or more networks from each other on different levels of the network stack. Data flow from one to another network can be allowed by a rule based policy enforced by these network components. The most common operation scenario of these network components is the separation between an internal and an external network. Therefore in this document this scenario is described. However also internal and external networks may not be considered necessarily as single networks but can also be a group of further networks which appear only as a single network to the TOE.

The secunet(wall comprises a solution set of Linux-based firewall components that enable the controlled transfer of data on a defined interface between internal and external networks or between segments of an internal network. This functionality is performed by the so-called Packet Filter, a part of the TOE. This packet filter enforced the Packet filter rules, defined by the administrator.

These filtering rules are configured and managed on a separated management system which is part of the TOE environment. Monitoring and logging (further referenced as auditing) takes place via a central journald logging service. This service must be installed on a machine in the management network.

The functionalities of the protective systems can be adapted to the required levels by the management system.

The secunet(wall provides functionality for packet filtering. This packet filtering is performed based on the information available at OSI layer 3 and layer 4 (IP and TCP or USP layer in the TCP/IP model). The functionality for packet filtering is part of the Linux operating system. The secunet(wall supports IPv4 [4] and IPv6. IPv6 is not part of the TOE. The secunet(wall also supports LDAP. LDAP is not part of the TOE.

The TOE is further capable of executing additional software which can further enhance the capabilities of the secunet(wall by offering additional functionality on top of the packet filtering functionality of the TOE. This additional software must be provided in the form of a systemd-nspawn software container. The TOE is capable of verifying the authenticity and integrity of this software container. I.e. the container must be signed. Further the TOE only supports one container running at the same time. However the functionality provided by this container is not in the scope of the TOE.

The following figure shows the physical setup of the TOE

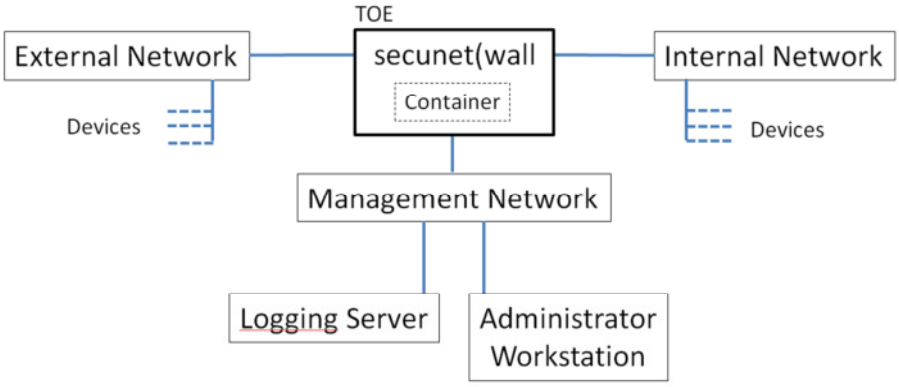


Figure 1 TOE environment

The TOE major security features are the following:

- The TOE enforces the Packet Filter information flow policy. This policy ensures that the TOE will only forward data from and to the internal network if the rules of the information flow policy allows it.
- The TOE collects audit data and sends it to a dedicated machine in the management network in order to identify attempts to violate a policy.
- The TOE is capable of performing management functions such as modification of networks filter traffic rules and configuration data.
- The TOE enforces the identification and authentication of an administrator before any management function can be performed.
- The TOE ensures the authenticity and integrity of a container running on the TOE upon container deployment and on every start of the container

The following security services are not part of the TOE and are thus to be provided by the IT environment:

- The IT environment provides an NTP service which provides reliable timestamps.
- The IT environment provides an auditing service which receives the TOE audit messages.
- The generation of the rules of the Packet Filter information flow policy and the configuration data takes place in the IT environment.

After start-up of the TOE and a secure initialisation process the TOE reads its configuration data from the local file system in the TOE system start-up process. The configuration data is the human readable content of the configuration file. The configuration data comprise IP address- and network interface definition, static routes and other system parameters. If no configuration data is available on start-up the TOE will not start-up automatically.

### 1.2.2 Required non TOE hardware/software/firmware

The TOE is delivered to the customer as software only on an installation medium (USB-Stick) from where it can be installed onto the customers own machines by either the customer or a secunet employee.

The TOE is tested and thus shall be operated on one of the following hardware:

- Fujitsu PRIMERGY RX 1330-M4 (Model: RX1330 M4 LFF or RX1330 M4 SFF)
- Syslogic COMPACT81-S (Model: SDB/OEMS81120-SBC1)

This hardware is not part of the TOE but secunet offers to forward the customers hardware purchase order to the hardware vendor.

The TOE has the following minimal requirements concerning the physical machine it runs on:

- Intel i686 compatible CPU
- 256 MB RAM
- three 1Gbit Ethernet Interfaces
- storage such as hard drive
- USB Controller
- Keyboard, Display, power support

## 1.3 TOE Description

### 1.3.1 Physical scope of the TOE

The TOE is a software product which runs on a hardware provided by secunet. It consists of several components that run in both kernel space and user space on the Linux operating system.

The following components are part of the kernel space:

- Packet Filter
- Management of rules of the Packet Filter information flow policy

The following components are part of the user space:

- Container authentication mechanism.
- Audit data collection
- Identification and authentication of the administrator

All delivery parts are listed in the following table:

| Delivered TOE parts | Version | Remarks |
|---|---|---|
| **secunet(wall** | Version 6.0.1 | software |
| **documentation** | Version 1.0 | electronic form (on CD and included in software) |

Table 1: Scope of TOE delivery

The TOE is delivered to the customer as software only on an installation medium (USB-Stick) and on CD (documentation).

### 1.3.2 Logical scope of the TOE

The following figure shows an overview of the TOE scope. The TOE scope inside the bigger Linux OS frame is highlighted.

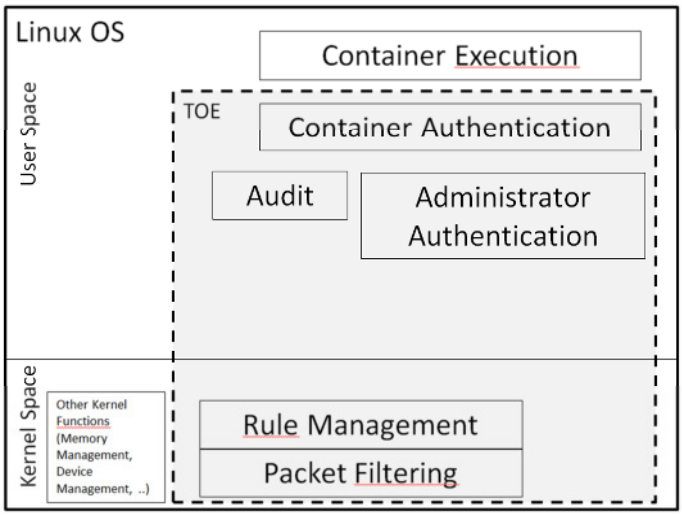


Figure 2 Toe Scope

#### 1.3.2.1 Information Flow Protection

The TOE enforces the Packet Filter information flow policy. This policy ensures that the TOE will only forward data from and to the internal network if the rules of the information flow policy allow it. Therefor the TOE implements the policy by providing routing functionality on the network layer (IP) and transport layer (TCP/UDP/ICMP). In order to apply the rules the TOE assesses the information from the IP and TCP/UDP/ICMP-Header (where applicable).

#### 1.3.2.2 Identification and Authentication

The Packet Filter information flow policy can be updated by an authenticated administrator. Before any management function can be performed the TOE verifies the identity of this administrator. Therefor the administrator must supply a username and a password which are verified by the TOE. The password is compared to a hash stored in a database in the TOE´s local filesystem.

#### 1.3.2.3 Management

The TSF is capable of performing the following management functions:

- Modification of rules of the Packet Filter information flow policy
- Modification of configuration data

The rules which form the Packet Filter information flow policy are created externally by use of various tools (e.g. the secunet(wall Builder).

The TOE is initialized with a strict rule set where everything is dropped (“dropping” in the contexts means, the packet is not transferred and no error message is returned to the sender).

#### 1.3.2.4 Container Authentication

The TOE ensures the authenticity and integrity of a software container which is deployed on the TOE. To achieve this it verifies a cryptographic signature supplied with the container. This signature is verified against a public key stored in the TOE´s local filesystem. Additionally on every start of the soft-

ware container the TOE verifies the authenticity of the “static” container parts in the same way. Note that some components of the container may change during execution such as configuration or log files. Therefore the TOE can only verify the “static” parts of the container which do not change over time (such as executables).

#### 1.3.2.5 Audit Data

The TOE collects audit data and sends it to a dedicated machine in the management network (see Figure 1) in order to identify attempts to violate a policy, container verification failures or unsuccessful administrator authentication attempts. This allows administrators to inspect the current state of the TOE or to view previous audit records. The TOE generates audit records for

- startup and shutdown of the audit functions,
- datagrams received or sent through a network components network interfaces if they match configured patterns,
- successful and unsuccessful administrator authentication attempts,
- Startup and shutdown of the hosted container and the result of the container integrity verification.

#### 1.3.2.6 Components

The secunet(wall Packet Filter consists of several components which are either part of the Linux kernel or user space. Table 2 shows which components are parts of the TOE and which are part of the IT environment.

| - | IT environment | TOE |
|---|---|---|
| **Kernel Space** | process management<br>memory management<br>device drivers | Packet Filter<br>Management of rules |
| **User Space** | Secure transport mechanism for configuration data and audit data.<br>Management (Configuration Tool) | Container authentication<br>Administrator Authentication<br>Audit mechanism |

Table 2: secunet(wall Packet Filter components

# 2 CONFORMANCE CLAIM

## 2.1 CC Conformance Claim

This Security Target and the TOE claim conformance to part 2 and part 3 of Common Criteria ([1] and [2]), Version 3.1 Revision 5:

## 2.2 PP and security requirement package claim

This Security Target does neither claim conformance to a Protection Profile nor to a security requirement package.

## 2.3 CC Conformance Claim Rationale

As this Security Target does neither claim conformance to a Protection Profile nor to a security requirement package a conformance claim rationale is not necessary.

## 2.4 Package Claim

This Security Target claims conformance to the assurance package EAL4 augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5.

ALC_FLR.2 adds flaw remediation procedures. ASE_TSS.2 required a brief overview on the architectural security functionality in the Security Target. AVA_VAN.5 adds advanced methodical vulnerability analysis assuming an attacker with a high attack potential.

# 3 SECURITY PROBLEM DEFINITION

This chapter introduces the security problem definition of the TOE. This comprises:

- The assets which have to be protected by the TOE.
- The subjects which are interacting with the TOE.
- The assumptions which have to be made about the environment of the TOE.
- The threats which exist against the assets of the TOE
- The organisational security policies the TOE has to comply to.

## 3.1 Assets

The following assets need to be protected by the TOE and its environment:

| Asset | Description |
|---|---|
| **TSF Data** | TSF data stored on the TOE which are necessary for its own operation. This includes packet filter rules and configuration data. |
| **Resources** | The resources in the connected networks that the TOE components are supposed to protect. The resources are outside the TOE components. |
| **Container** | The authenticity and integrity of the software container. |
| **Container verification key** | The public key that is used to verify the authenticity of the deployed container. |
| **Audit data** | Audit data transmitted from the network components to the management machine. |
| **Administrator password** | The hash of the administrator´s password is stored on the TOE´s file system. The password supplied by the administrator is hashed and compared to this hash on each authentication attempt of the administrator. |

Table 3: Assets

## 3.2 Subjects

The following subjects interact with the TOE.

| Subjects | Description |
|---|---|
| **Administrator** | The administrator of a network component is the person that has complete trust with respect to all policies implemented by the TSF. He or she is in charge of installing and configuring the TOE as well as performing the management functions of the TOE. |
| **User** | Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE. A goal of a user may be to access or modify sensitive information by sending IP packets to or receiving from the components of the TOE. This includes attacks from the protected networks behind the network components as well as attacks from outside those networks. Attackers with a high attack potential are assumed. |

Table 4: TOE Subjects

## 3.3 Assumptions

The following assumptions are made about the IT environment of the TOE to ensure the secure operation of the TOE.

| Assumption | Description |
|---|---|
| **A.Environment** | The TOE is used in a controlled environment. Specifically it is assumed:<br>That only the administrator gains physical access to the TOE,<br>That the administrator handles the authentication data with care, specifically that he will keep it secret and can use it in a way that nobody else can read it. |
| **A.NoEvil** | The administrator of the TOE is non hostile, well trained and knows the documentation of the TOE.<br>The administrator is responsible for the secure operation of the TOE and its environment. |
| **A.InformationFlow** | No information can flow between the internal and external networks unless it passes through the TOE. |
| **A.Configuration** | The network components (TOE and application) are configured in a secure manner. Specifically it is assumed that no incoming connections are accepted except protected data (SSH, [3]) from the management machine. |
| **A.Timestamp** | The IT environment provides reliable timestamps (NTP server). |
| **A.Management** | Access to the management interface is only possible from a distinct management network which is physically separated from both the internal and external network. |
| **A.Audit** | The IT environment provides a audit server and a means to present a readable view of the audit data. |
| **A.ContainerSigning** | The creation of the public key pair that is used to sign and verify the container takes place in a secure environment. Also the signing of the container with the public key is performed in a secure environment. |
| **A.TrustworthyContainer** | The container content is trustworthy and does not con- |

| | |
|---|---|
| | tain any unwanted functionality. |

Table 5: Assumptions

## 3.4 Threats

The following threats have to be countered by the TOE. Hereby attackers with a high attack potential are assumed.

| Threat | Description |
|---|---|
| **T.Bypass** | A user might attempt to bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected network.<br>E. g., a user might send non-permissible data through the TOE in order to gain access to resources in protected network by sending IP packets to circumvent filters. This attack may happen from outside the protected network. |
| **T.Weakness** | A user might gain access to the TOE in order to read, modify or destroy TSF data by sending IP packets to the TOE and exploiting a weakness of the protocol used. This attack may happen from outside and inside the protected network. A user might also try to access sensitive data of the TOE via its management interface. |
| **T.NoAuthentication** | An unauthenticated user may attempt to bypass the security functions of the TOE and gain unauthenticated access to resources in other connected networks or security sensitive data on the TOE. |

Table 6: Threats

## 3.5 Organisational security policies

| OSP | Description |
|---|---|
| **OSP.Container** | The TOE shall be capable of running a systemd-nspawn container. The authenticity and integrity of this container must be ensured by the TOE. |
| **OSP.Passwords** | The password used by the administrator must be of sufficient quality and kept secret. |

# 4 STATEMENT OF SECURITY OBJECTIVES

This chapter describes the security objectives for the TOE (in chapter 4.1), the security objectives for the operational environment of the TOE (in chapter 4.2) and contains the security objectives rationale.

## 4.1 Security Objectives for the TOE

The following security objectives have to be met by the TOE

| Policy | Description |
|---|---|
| **O.Management** | The TOE must verify the identity and authenticity of an administrator before any management function can be performed. It must provide means to deal with failed login attempts. The TOE must provide the necessary management functions in order to modify the configuration data or the traffic filter rules. |
| **O.Filter** | The TOE must filter the incoming and the outgoing data traffic of all data between all connected networks according to the rule set. |
| **O.Audit** | The TOE must provide an audit trail of security-related events. |
| **O.Container** | The TOE must ensure the authenticity and integrity of a container deployed on the TOE. |

Table 7: Security Objectives for the TOE

## 4.2 Security Objectives for the Operational Environment

The following security objectives have to be met by the operational environment of the TOE.

| Policy | Description |
|---|---|
| **OE.Environment** | The TOE is used in a controlled environment. Specifically it must be enforced:<br>■ That only the administrator gains physical access to the TOE,<br>■ That the administrator handles the password associated with his or her account with care, choses a password with sufficient quality and keeps it secret. |
| **OE.NoEvil** | The administrator of the TOE shall be non-hostile, well trained and has to know and follow the documentation of the TOE.<br>The administrator is responsible for the secure operation of the TOE and its environment. |
| **OE.InformationFlow** | The administrator must assure that the packet filter components provide the only connection for the different networks. |
| **OE.Configuration** | The network components (TOE and application) must be configured to accept only protected data (SSH, [3]) from the management machine. |
| **OE.Timestamp** | The IT environment must provide reliable timestamps (NTP server). |
| **OE.Management** | Access to the management interface shall only be possible from a distinct management network which shall be physically separated from both the internal and external network. Also the machine used by the administrator to connect to the web interface and the server(-s) which receive and store the audit records from the TOE shall be located in this management network. |
| **OE.Audit** | The IT environment provides a Syslog server and a means to present a readable view of the audit data. |
| **OE.ContainerSigning** | The creation of the public key pair that is used to sign and verify the container must take place in a secure environment. Also the signing of the container with the public key must be performed in a secure environment. |
| **OE.TrustworthyContainer** | It must be ensured by the environment that the container content does not contain any unwanted functionality. |

Table 8: Security Objectives for the environment of the TOE

## 4.3 Security Objectives Rationale

The following table provides an overview for security objectives coverage. The following chapters provide a more detailed explanation of this mapping.

| | OE.Environment | OE.NoEvil | OE.InformationFlow | OE.Configuration | OE.Timestamp | OE.Management | OE.ContainerSigning | OE.TrustworthyContainer | OE.Audit | O.Filter | O.Audit | O.Management | O.Container |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.Environment | X | | | | | | | | | | | | |
| A.NoEvil | | X | | | | | | | | | | | |
| A.InformationFlow | | | X | | | | | | | | | | |
| A.Configuration | | | | X | | | | | | | | | |
| A.Timestamp | | | | | X | | | | | | | | |
| A.Management | | | | | | X | | | | | | | |
| A.ContainerSigning | | | | | | | X | | | | | | |
| A.TrustworthyContainer | | | | | | | | X | | | | | |
| A.Audit | | | | | | | | | X | | | | |
| T.Bypass | X | | X | | | X | | | | X | | | |
| T.Weakness | | | | X | | | | | X | | X | X | |
| T.NoAuthentication | | | | | | | | | | X | | X | |
| OSP.Container | | | | | | | | | | | | | X |
| OSP.Passwords | X | | | | | | | | | | | | |

Table 9: Security Objective Rationale

### 4.3.1 Countering the threats

The threat **T.Bypass** which describes that an attacker may bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected networks is countered by a combination of the objectives *OE.Management, OE.Environment, OE.InformationFlow* and *O.Filter*. The environmental objectives *OE.Environment* and *OE.InformationFlow* ensure that a user can neither interfere with the initial setup or the physical setup of the management machine or network components nor routes around the management machine or network components. Thus, all data pass through the TOE. *O.Filter* ensures that this data is always checked and filtered according to the policy. The environmental objective *OE.Management* ensures that data flow between the management machine and the network components only occurs in the separated management network, i.e. that sessions of users already authenticated cannot be taken over.

The threat **T.Weakness** which describes that an attacker may try to exploit a weakness of the protocol used in order to read, modify or destroy security sensitive data on the TOE is countered by a combination of the objectives *O.Audit, OE.Audit, OE.Configuration* and *O.Management*. *O.Audit* and *OE.Audit* ensure detection of attempts to compromise the TOE.

The threat **T.NoAuthentication** describes the situation that an unauthenticated user bypasses the security functions of the TOE and gets access to resources in other connected networks or security sensitive data on the TOE. Access to recources in connected networks is covered by the objective *O.Filter* which enforces a strict filtering policy. Every access not explicitly allowd is blocked by the TOE. The objective *O.Management* counters unauthenticated access to data on the TOE istself because it enforces the authentication of every administrator.

### 4.3.2 Covering the OSPs

The organisation security policy **OSP.Container** claims that a container must be protected in its authenticity and integrity. It is covered by *O.Container* which ensures that the authenticity and integrity is enforced.

The organisational security policy **OSP.Passwords** claims that passwords used by the administrators are of sufficient quality. This requirement is fulfilled by the objective for the environment *OE.Environment* which covers the objective for administrators to choose a password with sufficient quality and handle it secretly.

### 4.3.3 Covering the assumptions

The assumption **A.Environment** is covered by *OE.Environment* as directly follows.

The assumption **A.NoEvil** is covered by *OE.NoEvil* as directly follows.

The assumption **A.InformationFlow** is covered by *OE.InformationFlow* as directly follows.

The assumption **A.Configuration** is covered by *OE.Configuration* as directly follows.

The assumption **A.Timestamp** is covered by *OE.Timestamp* as directly follows.

The assumption **A.Audit** is covered by *OE.Audit* as directly follows.

The assumption **A.ContainerSigning** is covered by OE.ContainerSigning as directly follows.

The assumption **A.TrustworthyContainer** is covered by OE.TrustworthyContainer as directly follows.

# 5 STATEMENT OF SECURITY REQUIREMENTS

This chapter defines the security functional requirements (see chapter 5.1) and the security assurance requirements for the TOE (see chapter 5.3). No extended components are defined in this Security Target (see chapter 5.2).

The CC allows several operations to be performed on functional requirements: *refinement, selection, assignment*, and *iteration* are defined in paragraph C.4 of Part 1 of the CC [CC_Part1]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by the word “refinement” and by added/changed words are **in bold text**. In cases where words from a CC requirement were deleted, they are marked as ~~stroked out~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted as regular text inside square brackets (“[ ]”).

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments are denoted as *italic* text inside square brackets (“[ ]”).

The **iteration** operation is used when a component is repeated with varying operations. Iterations are denoted by showing a slash (“/”) and the iteration indicator after the component identifier.

## 5.1 Security functional requirements for the TOE

The TOE satisfies the SFRs delineated in the following table. The rest of this chapter contains a description of each component and any related dependencies.

| | |
|---|---|
| **Security audit (FAU)** | |
| **FAU_GEN.1** | Audit data generation |
| **Cryptographic Support (FCS)** | |
| **FCS_COP.1/RSA-verify** | Cryptographic Operation – RSA-verify |
| **FCS_COP.1/SHA** | Cryptographic Operation – SHA |
| **User data protection (FDP)** | |

| | |
|---|---|
| **FDP_IFC.1** | Subset information flow control |
| **FDP_IFF.1** | Simple security attributes |
| **FDP_ITC.2** | Import of user data with security attributes |
| **User identification (FIA)** | |
| **FIA_AFL.1** | Authentication failure handling |
| **FIA_UID.1** | Timing of identification |
| **FIA_UAU.1** | Timing of authentication |
| **Security management (FMT)** | |
| **FMT_MSA.1** | Management of security attributes |
| **FMT_MSA.3** | Static attribute initialisation |
| **FMT_SMF.1** | Specification of management functions |
| **FMT_SMR.1** | Security roles |
| **Protection of the TSF (FPT)** | |
| **FPT_STM.1** | Reliable time stamps |
| **FPT_TDC.1** | Inter-TSF basic TSF data consistency |

Table 10: Security Functional Requirements for the TOE

## 5.1.1 Security Audit

### 5.1.1.1 FAU_GEN.1 Audit data generation

| | |
|---|---|
| **FAU_GEN.1.1** | The TSF shall be able to generate an audit record of the following auditable events:<br>a) Start-up and shutdown of the audit functions;<br>b) All auditable events for the [not specified] level of audit; and<br>c) [*starting of network components; IP datagrams matching log filters in packet filter rules, user login attemps*] |
| **FAU_GEN.1.2** | The TSF shall record within each audit record at least the following information:<br>a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;<br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*]. |
| **Hierarchical to:** | No other components |
| **Dependencies:** | FPT_STM.1 Reliable time stamps |
| **Application Note:** | Please note if Syslogic COMPACT81-S hardware is used: Heavy load on the network device might impact audit data generation of the TOE.<br>Under heavy load the kernel still generates kernel messages and transfers them to the syslog component but the syslog component may miss some of these kernel messages.<br>In this case the syslog component generates audit data which only contain the information on how many kernel messages are missed in contrary to the detailed information of regular audit data. |

## 5.1.2 Cryptographic Support (FCS)

### 5.1.2.1 FCS_COP.1/SHA Cryptographic operation

| | |
|---|---|
| **FCS_COP.1.1/SHA** | The TSF shall perform [*hashing*] in accordance with a |

| | |
|---|---|
| | specified cryptographic algorithm [SHA-256 and *SHA-512*] and cryptographic key sizes [*none*] that meet the following: [*FIPS_180-4*]. |
| **Hierarchical to:** | No other components |
| **Dependencies:** | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |
| **Application Note:** | SHA-256 is used for Container authentication.<br>SHA-512 is used for Password hashing. |

#### 5.1.2.2 FCS_COP.1/RSA-verify Cryptographic operation

| | |
|---|---|
| **FCS_COP.1.1/RSA-verify** | The TSF shall perform [*verification of digital signatues*] in accordance with a specified cryptographic algorithm [*sha256withRSAEncryption OID 1.2.840.113549.1.1.11*] and cryptographic key sizes [*4096bit*] that meet the following: [*IETF RFC 8017 and FIPS_180-4*]. |
| **Hierarchical to:** | No other components |
| **Dependencies:** | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]<br>FCS_CKM.4 Cryptographic key destruction |

#### 5.1.2.3 FDP_IFC.1 Subset information flow control

| | |
|---|---|
| **FDP_IFC.1.1** | The TSF shall enforce the [*Packet Filter SFP*] on<br>[*Subjects: users (external entities) that send and/or receive information through the TOE to one another;*<br>*Information: data sent from one subject through the TOE to one another;*<br>*Operation: pass the data*]. |
| **Hierarchical to:** | No other components. |

| | |
|---|---|
| **Dependencies:** | FDP_IFF.1 Simple security attributes |
| **Application Note:** | The Packet Filter SFP is given in FDP_IFF. The subject definition in FDP_IFC.1.1 belongs to a former CC version. Thus the subjects are identical to the administrator defined in the subjects definition in chap. 3.3. |

#### 5.1.2.4 FDP_IFF.1 Simple security attributes

| | |
|---|---|
| **FDP_IFF.1.1** | The TSF shall enforce the [*Packet Filter SFP*] based on the following types of subject and information security attributes:<br>[*Subjects: users (external entities) that send and/or receive information through the TOE to one another;*<br>*Subject security attributes: none;*<br>*Information: data sent from one subject through the TOE to one another;*<br>*Information security attributes: source address of subject, destination address of subject, transport layer protocol, interface on which the traffic arrives and departs, port, time*]. |
| **FDP_IFF.1.2** | The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*Subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information policy rules*]. |
| **FDP_IFF.1.3** | The TSF shall enforce the [*reassembly of fragmented IP datagrams before inspection*]. |
| **FDP_IFF.1.4** | The TSF shall explicitly authorise an information flow based on the following rules: [*none*]. |
| **FDP_IFF.1.5** | The TSF shall explicitly deny an information flow based on the following rules:<br>■ [*The TOE shall reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject does not belong to the network associated with the interface (spoofed packets);*<br>■ *The TSF shall drop IP datagrams with the source routing option;* |

| | |
|---|---|
| | ■ *The TOE shall reject fragmented IP datagrams which cannot be reassembled completely within a bounded interval*]. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | FDP_IFC.1 Subset information flow control<br>FMT_MSA.3 Static attribute initialisation |
| **Application Note:** | The subject definition in FDP_IFF.1.1 belongs to a former CC version. Thus the subjects are identical to the subjects defined in the external entities definition in chap. 3.3. |

#### 5.1.2.5 FDP_ITC.2 Import of user data with security attributes

| | |
|---|---|
| **FDP_ITC.2.1** | The TSF shall enforce the [*container deployment SFP*] when importing user data, controlled under the SFP, from outside of the TOE. |
| **FDP_ITC.2.2** | The TSF shall use the security attributes associated with the imported user data. |
| **FDP_ITC.2.3** | The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received. |
| **FDP_ITC.2.4** | The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data. |
| **FDP_ITC.2.5** | The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [*none*]. |
| **Hierarchical to:** | No other components |
| **Dependencies:** | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]<br>[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]<br>FPT_TDC.1 Inter-TSF basic TSF data consistency |

## 5.1.3 User identification (UID)

#### 5.1.3.1 FIA_AFL.1 Authentication failure handling

| | |
|---|---|
| **FIA_AFL.1.1** | The TSF shall detect when [*1*] unsuccessful authentication attempts occur related to [*login*]. |
| **FIA_AFL.1.2** | When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*delay the next login attempt for 3 seconds*]. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | FIA_UAU.1 Timing of authentication |

#### 5.1.3.2 FIA_UAU.1 Timing of authentication

| | |
|---|---|
| **FIA_UAU.1.1** | The TSF shall allow [*all actions except for administrative actions as specified by FMT_SMF.1*] on behalf of the user to be performed before the user is identified. |
| **FIA_UAU.1.2** | The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. |
| **Hierarchical to:** | No other components |
| **Dependencies:** | FIA_UID.1 Timing of identification |

#### 5.1.3.3 FIA_UID.1 Timing of identification

| | |
|---|---|
| **FIA_UID.1.1** | The TSF shall allow [*all actions except for administrative actions as specified by FMT_SMF.1*] on behalf of the user to be performed before the user is identified. |
| **FIA_UID.1.2** | The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | No dependencies. |

#### 5.1.3.4 Security management (FMT)

#### 5.1.3.5 FMT_MSA.1 Management of security attributes

| | |
|---|---|
| **FMT_MSA.1.1** | The TSF shall enforce the [*Packet Filter SFP*] to restrict the ability to [modify] the security attributes [*network traffic filter rules and configuration data*] to [*the role administrator*]. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | [FDP_ACC.1 Subset access control, or<br>FDP_IFC.1 Subset information flow control]<br>FMT_SMR.1 Security roles<br>FMT_SMF.1 Specification of Management |

#### 5.1.3.6 FMT_MSA.3 Static attribute initialization

| | |
|---|---|
| **FMT_MSA.3.1** | The TSF shall enforce the [*Packet Filter SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP. |
| **FMT_MSA.3.2** | The TSF shall allow the [*no roles*] to specify alternative initial values to override the default values when an object or information is created. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | FMT_MSA.1 Management of security attributes<br>FMT_SMR.1 Security roles |

#### 5.1.3.7 FMT_SMF.1 Specification of management functions

| | |
|---|---|
| **FMT_SMF.1.1** | The TSF shall be capable of performing the following management functions: [<br>■ *Modification of the rules of the Packet Filter information flow policy,*<br>■ *Modification of configuration data*]. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | No dependencies. |

#### 5.1.3.8 FMT_SMR.1 Security roles

| | |
|---|---|
| **FMT_SMR.1.1** | The TSF shall maintain the roles [*administrator*]. |
| **FMT_SMR.1.2** | The TSF shall be able to associate users with roles. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | FIA_UID.1 Timing of identification |

### 5.1.4 Protection of the TSF (FPT)

#### 5.1.4.1 FPT_STM.1 Reliable time stamps

| | |
|---|---|
| **FPT_STM.1.1** | The TSF shall be able to provide reliable time stamps. |
| **Hierarchical to:** | No other components. |
| **Dependencies:** | No dependencies. |

*Application Note: The TOE provides reliable timestamps to the hosted container*

#### 5.1.4.2 FPT_TDC.1 Inter-TSF basic TSF data consistency

| | |
|---|---|
| **FPT_TDC.1.1** | The TSF shall provide the capability to consistently interpret [*the container*] when shared between the TSF and another trusted IT product. |
| **FPT_TDC.1.2** | The TSF shall use [*the signature attached to the container*] when interpreting the TSF data from another trusted IT product. |
| **Hierarchical to:** | No other components. |

| | |
|---|---|
| **Dependencies:** | No dependencies. |

## 5.2 Extended Components definition

No extended components are defined in this Security Target.

## 5.3 Security assurance requirements for the TOE

The following table lists the chosen evaluation assurance components for the TOE.

| Assurance Class | Assurance Components |
|---|---|
| **ASE** | ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, **ASE_TSS.2** |
| **ADV** | ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3 |
| **AGD** | AGD_OPE.1, AGD_PRE.1 |
| **ALC** | ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1 **ALC_FLR.2**, ALC_LCD.1, ALC_TAT.1 |
| **ATE** | ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2 |
| **AVA** | **AVA_VAN.5** |

Table 11: Chosen Evaluation Assurance Requirements

These assurance components represent EAL 4 augmented by the component marked in bold text. The complete text for these requirements can be found in [2].

## 5.4 Security Requirements Rationale

### 5.4.1 TOE functional requirements rationale

| | O.Filter | O.Audit | O.Management | O.Container |
|---|---|---|---|---|
| **FAU_GEN.1** | | X | | |
| **FCS_COP.1/RSA-verify** | | | | X |
| **FCS_COP.1/SHA** | | | X | X |
| **FDP_IFC.1** | X | | | |
| **FDP_IFF.1** | X | | | |
| **FDP_ITC.2** | | | | X |
| **FIA_AFL.1** | | | X | |
| **FIA_UID.1** | | | X | |
| **FIA_UAU.1** | | | X | |
| **FMT_MSA.1** | | | X | |
| **FMT_MSA.3** | X | | | |
| **FMT_SMF.1** | | | X | |
| **FMT_SMR.1** | | | X | |
| **FPT_STM.1** | | X | | X |
| **FPT_TDC.1** | | | | X |

Table 12: Coverage of Security Objective for the TOE by SFRs

The security objective **O.Filter** is met by a combination of FDP_IFC.1, FDP_IFF.1 and FMT_MSA.3. FDP_IFC.1 and FDP_IFF.1 describe the information flow policy. Together, the SFRs describe how the Packet Filter information flow policy apply. FMT_MSA.3 defines that the TOE has to provide restrictive default values for the Packet Filter SFP (information flow policy) attributes. The SFRs are therefore sufficient to satisfy the objective **O.Filter** and mutually supportive.

The security objective **O.Audit** is met by FAU_GEN.1 and FPT_STM.1. FAU_GEN.1 describes when and what kind of audit data is generated. FPT_STM.1 covers the provision of reliable time stamps needed to produce reliable audit records**.**

The security objective **O.Management** is met by FMT_SMF.1, FMT_MSA.1, FIA_UID.1, FIA_UAU.1, FIA_AFL.1 and FMT_SMR.1. FMT_SMF.1 describes the minimum set of management functionality, which has to be available. FMT_MSA.1 defines, which roles are allowed to administer the security attributes of the TOE. FIA_UID.1 and FIA_UAU.1 require each user to be identified and authenticated before allowing any relevant actions on behalf of that user. The password verification uses the SHA512 hashing mechanism covered by FCS_COP.1/SHA. Further the objective requires that the TOE will at least maintain the role administrator. This is defined in FMT_SMR.1, which defines the role. Failure handling regarding authentication is covered by FIA_AFL.1.

The security objective **O.Container** is met by FDP_ITC.2 and FPT_TDC.1. The SFR FDP_ITC.2 covers the import of user data with an attached signature. FPT_TDC.1 requires the TOE to verify the signature attached to the container. The cryptographic mechanisms for the verification are covered by FCS_COP.1/RSA-verify and FCS_COP.1/SHA.

### 5.4.2 Fulfilling the SFR dependencies

The following table shows that all dependencies are met.

| SFR | Dependencies | Fulfilled by |
|---|---|---|
| **FAU_GEN.1** | FPT_STM.1 | FPT_STM.1 |
| **FCS_COP.1/RSA-verify** | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] | **not fulfilled, but justified**<br>The public key is installed as part of the regular installation process. |
| | FCS_CKM.4 Cryptographic key destruction | **not fulfilled, but justified**<br>Because the cryptographic key used by FCS_COP.1/RSA-verify is a public RSA key which does not to be protected against disclosure, a secure destruction is not necessary. |
| **FCS_COP.1/SHA** | [FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] | **not fulfilled but justified**<br>The algorithm does not contain a cryptographic key. |

| | | |
|---|---|---|
| | FCS_CKM.4 Cryptographic key destruction | **not fulfilled but justified**<br>The algorithm does not contain a cryptographic key. |
| **FDP_IFC.1** | FDP_IFF.1 | FDP_IFF.1 |
| **FDP_IFF.1** | FDP_IFC.1<br>FMT_MSA.3 | FDP_IFC.1<br>FMT_MSA.3 |
| **FDP_ITC.2** | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | **not fulfilled, but justified**<br>Access control is provided by the environment because the signing of the container is restricted to authorised personnel only and takes place in the secure environment (see OE.ContainerSigning) |
| | [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] | **not fulfilled, but justified**<br>The establishment of a trusted communication path is not necessary because the data flows only to the TOE but not in the opposite direction (deployment of container). The container is signed with the signers private key which allows the TOE to verify the authenticity of the container. No data flows in the opposite direction, therefore the TOE does not need to authenticate itself. |
| | FPT_TDC.1 Inter-TSF basic TSF data consistency | FPT_TDC.1 |
| **FIA_AFL.1** | FIA_UAU.1 | FIA_UAU.1 |
| **FIA_UID.1** | No dependencies. | - |
| **FIA_UAU.1** | FIA_UID.1 | FIA_UID.1 |
| **FMT_MSA.1** | [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] | FDP_IFC.1 |
| | FMT_SMR.1 Security roles | FMT_SMR.1 |

| | | |
|---|---|---|
| | FMT_SMF.1 Specification of Management | FMT_SMF.1 |
| **FMT_MSA.3** | FMT_MSA.1 | FMT_MSA.1 |
| | FMT_SMR.1 | FMT_SMR.1 |
| **FMT_SMF.1** | No dependencies. | - |
| **FMT_SMR.1** | FIA_UID.1 | FIA_UID.1 |
| **FPT_STM.1** | No dependencies. | - |
| **FPT_TDC.1** | No dependencies. | - |

Table 13: Fulfilling the SFR dependencies

### 5.4.3 Security assurance requirements rationale

The TOE claims compliance to EAL4 level of assurance augmented by ALC_FLR.2, ASE_TSS.2 and AVA_VAN.5. As described in [2], the level EAL4 indicates that the product is methodically designed, tested, and reviewed.

The Assurance requirements for the vulnerability analysis class have been augmented by AVA_VAN.5 which requires an advanced methodical vulnerability analysis assuming a ‘High’ attack potential.

The Assurance requirements for the Security Target Evaluation have been augmented by ASE_TSS.2 which requires an architectural design summary in the Security Target which describes how the TOE protects itself against interference, logical tampering and bypassing of security functions.

Additionally the assurance requirements for life cycle support have been augmented by ALC_FLR.2 (flaw reporting procedures) to account for regular bug fixes for the TOE.

# 6 TOE SUMMARY SPECIFICATION

## 6.1 TOE security functionality

### 6.1.1 SF1 Information Flow Protection

SF1.1: The TSF implements the information flow control on the network layer for the IP protocol and on the transport layer for the protocols TCP, UDP and ICMP. In order to define packet filter rules the TSF provides packet filter criteria and packet filter actions. The packet filter criteria are defined by the following parameters:

- source address of the IP header
- destination address of the IP header
- transport layer protocol
- interface on which traffic arrives and departs
- port (TCP/UDP)
- time

**The packet filter actions are:**

- accept (permit)
- reject (deny and send error message to the sender)
- drop (deny without sending an error message to the sender)

In order to apply the packet filter rules the TOE uses the information in the IP header on the network layer and the TCP/UDP/ICMP-Header in the transport layer where applicable.

This aspect covers FDP_IFC.1.

SF1.2: The TSF reassembles IP datagrams before further processing is performed. IP datagrams which cannot be reassembled in a predefined span of time are dropped.

This aspect covers FDP_IFF.1.

SF1.3: The TSF drops packets with spoofed source- or destination-IP addresses. Packets with source routing options are also dropped.

This aspect also covers FDP_IFF.1.

### 6.1.2 SF2 Management

SF2.1: The TSF is capable of performing the following management functions:

- Modification of the rules of the Packet Filter information flow policy,
- Modification of configuration data,

This aspect covers FMT_SMF.1.

SF2.2: The Linux operating system supports more than one user role, but only the administrator role is allowed to modify the security attributes network traffic filter rules and configuration data. The administrator can log in at the TOE locally by supplying username and password. The TOE then performs the identification and authentication. Therefore it verifies the supplied password by hashing it 5000 times and comparing it to the stored hash of the original password. To protect against brute-force login attacks, after each unsuccessful login attempt further authentication attempts are delayed by 3 seconds.

This aspect covers FCS_COP.1/SHA, FIA_AFL.1, FIA_UID.1, FIA_UAU.1, FMT_MSA.1 and FMT_SMR.1.

SF2.3: The TOE is initialized with a strict packet filter rule set. All packets received packets are dropped.

This aspect covers FMT_MSA.3.

### 6.1.3 SF3 Container Authentication

SF3.1: The TOE verifies the authenticity and integrity of a software container deployed on the TOE. Therefor the TOE uses a signature provided with the container itself. The public key which is needed to verify this signature is located on the local filesystem of the TOE itself. Only if the signature is valid (the container file has been signed with the corresponding private key) the TOE allows the deployment of the software container. On every start of the container software the same mechanism verifies the authenticity and integrity of the container.

This aspect covers FCS_COP.1/RSA-verify, FCS_COP.1/SHA, FDP_ITC.2 and FPT_TDC.1.

SF3.2: The TOE provides the container with reliable timestamps.

This aspect covers FPT_STM.1.

### 6.1.4 SF4 Security Audit

SF4.1: The TSF generates audit records for

- start-up and shutdown of the audit functions
- datagrams received or sent through a network interface of the TOE if they match configured patterns defined in the audit configuration
- successful and unsuccessful administrator authentication attempts

Audit records sent to a dedicated server in the management network which further processes the audit records.

This aspect covers FAU_GEN.1

SF4.2: Each record includes:

- Time and Date of the occurred event

For entries that cover network datagrams additionally the following is included into the audit records:

- Affected network component
- Subject identity (source IP)
- Type of event
- Affected interface
- Direction
- Action (accept, drop or reject)
- Optional depending on the protocol: IP addresses and ports

For audit records which cover the successful or unsuccessful authentication attempts additionally the following is included:

- Username
- User ID

This aspect covers FAU_GEN.1 and FPT_STM.1.

Application Note: Please note if Syslogic COMPACT81-S hardware is used: Heavy load on the network device might impact audit data generation of the TOE. Under heavy load the kernel still generates kernel messages and transfers them to the syslog component but the syslog component may miss some of these kernel messages. In this case the syslog component generates audit data which only contain the information on how many kernel messages are missed in contrary to the detailed information of regular audit data. This state is only temporary. After the heavy load is not present anymore the full logging functionality is restored. This does not lead to a non-deterministic behaviour of the logging functionality. The reduced Logging does not violate SF4 Security Audit. In fact syslog messages of missed kernel messages indicate that the TOE environment reaches the boundary according FAU_GEN.1 due to heavy load on network device.

## 6.2 Mapping between Security Functionality (SF) and Security Functional Requirements (SFRs)

| SFR | TOE Security Functionality | | | |
|---|---|---|---|---|
| | SF1 Information Flow Protection | SF2 Manage-ment | SF3 Container Authentication | SF4 Security Audit |
| FAU_GEN.1 | | | | X |
| FCS_COP.1/RSA-verify | | | X | |
| FCS_COP.1/SHA | | X | X | |
| FDP_IFC.1 | X | | | |
| FDP_IFF.1 | X | | | |
| FDP_ITC.2 | | | X | |
| FIA_AFL.1 | | X | | |
| FIA_UID.1 | | X | | |
| FIA_UAU.1 | | X | | |
| FMT_MSA.1 | | X | | |
| FMT_MSA.3 | | X | | |
| FMT_SMF.1 | | X | | |
| FMT_SMR.1 | | X | | |
| FPT_STM.1 | | | X | X |
| FPT_TDC.1 | | | X | |

## 6.3 Self-Protection against Interference and Logical Tampering

The TOE has a hardened kernel which encompasses:

- Data memory is non-executable
- Code memory is non-writable
- Address space layout randomization
- Improved chroot restrictions to prevent privilege escalations
- Extended syscall Auditing (i.e. chroot, chdir, ptrace, mount ...)
- Sysctl sealing to prevent modifications after sealing
- Module load sealing to prevent module loads after sealing
- Capability based privilege separation

The TOE also has a hardened userspace with the following security measures:

- Stack-Smashing-Protection, Jump-Over-Stack-Checks via compiler flags to detect stack attacks
- Common string/mem functions in the libc have extended bound-checks to detect buffer overflows before they happen (str*cpy(), *printf(), *scanf(), memcpy(), ... )
  The root filesystem is mounted as read-only and therefore cannot be modified by an attacker
- Only configuration and log files in the the /etc and /var directories are writeable by the TOE.
- The /etc, /tmp directories are mounted non-executable
- Firewall rulesets are secure by Linux capabilities. Only users with the capability CAP_NET_ADMIN can change firewall rulesets.

## 6.4 Self-Protection against Bypass

Because the TOE is a firewall system, there can be no bypassing if it is installed properly. This is reflected by the assumption A.InformationFlow. The TOE protects itself against by-passing of security functions by enforcing a strict filtering policy. The TOE also enforces that all management functoins can only be performd by an authenticated user.

# 7 GLOSSARY AND ACRONYMS

| | Definition |
|---|---|
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik |
| **NTP** | Network Time Protocol |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SAR** | Security Assurance Requirement |
| **SSH** | Secure Shell |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |

# 8 REFERENCES

**Common Criteria**

[1] Common Criteria for Information 2: Security Functional Components; Version 3.1, Revision 5, CCMB-2017-04-002

[2] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 5, CCMB-2017-04-003

**Cryptography**

[3] RFC4253, SSH Transport Layer Protocol, http://www.ietf.org/rfc/rfc4253.txt

[4] RFC 791, Internet Protocol, http://www.ietf.org/rfc/rfc791.txt

[FIPS_180-4] FIPS PUB 180-4, Secure Hash Standard, National Institute of Standards and Technology, 2012-03.

[IETF RFC 8017] RFC 8017, PKCS #1: RSA Cryptography Specifications Version 2.2