Security Target for secunet SBC Container

secunet Security Networks AG
Kurfürstenstraße 58,
45138 Essen
Internet: www.secunet.com

History

Version	Date	Changes	Remarks
0.9	26.09.2021	Draft Security Target based on BSI-DSZ-CC-1089	
0.92	06.10.2021	Changes due to BSI comments	
1.0	06.04.2022	Final Version	
1.1	26.04.2022	Finale Version -16	

Last Version: 1.1 (26.04.2022)

Table of Contents

1. ST Introduction

1.1. ST-Reference

Title:	Security Target for secunet SBC Container
Document Version:	1.1
Document Date:	26.04.2022
Document State:	Final
ST Registration:	BSI-DSZ-CC-1089-V2
Certification body:	Bundesamt für Sicherheit in der Informationstechnik (BSI)
CC-Version	3.1 (Revision 5)
Assurance level:	EAL4 augment by ALC_FLR.2, AVA_VAN.5, ASE_TSS.2
Author:	Hendrik Dettmer on behalf of secunet AG
TOE Name.	secunet SBC Container
TOE Version	4.2.10-16
Keywords:	Session Border Controller, SBC, SBC Container, Gateway, VoIP, SIP, Packet filter

This Security Target claims conformance with the following documents:

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology (CEM), Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

1.2. TOE Overview

1.2.1. Usage and Major Security features

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

The TOE is the secunet SBC (Session Border Controller) Container, a Linux systemd-nspawn container which must be deployed on a Linux operating system. A session border controller in general is a device deployed at the border of a network segment to exert control over the signaling and the audio and video media streams involved in setting up, conducting, and tearing down audio and video calls or other interactive media communications. This communication is called VoIP (Voice over IP). However, it is common to also include video communication in this definition, so VoIP will be used in this document as a generalization of audio and video real-time communication.

The secunet SBC Container is a software TOE which must be deployed on a hardened Linux operating system platform, secunet Wall at least version 6.1.0 or a hardened centOS at least version 7.9. This operating system platform protects the integrity of the TOE. The main purpose of the secunet SBC Container is the initiation of a secure SIP session (also called signaling) and media communication streams such as RTP or SRTP. It allows the secure media communication between different companies or separated departments inside a single company and enforces an optimal SIP and media stream interoperability.

The secunet SBC Container must be deployed on a Linux system which routes all necessary traffic to it. This system can also contain a firewall, which protects the Session Border Controller software and prevents unwanted data flows from or to the protected network. The secunet SBC Container itself allows a separation between different VoIP networks as well as a connection between them and thus becomes the access point for internal VoIP networks.

To protect the internal network, the TOE performs data inspection and filtering on several protocol levels.

This includes the possibility to configure the TOE to filter SIP methods so that the registration of devices is only possible from the internal network. OPTIONS requests can be filtered or answered by the TOE such that IP addresses, which provide information about devices in the internal network, are not visible outside of the protected network.

The TOE can be configured so that the SIP header fields are stripped of IP addresses that could provide insights about the internal network structure and devices. Information from external sources shall be well-formed to prevent attackers from using malformed data to exploit local network devices.

If configured, the SDP message body included in SIP requests is filtered to only allow specific content-types and codecs to reduce the attack surface.

Out-of-dialog SIP requests from the external network per time period can be limited to a specific value in order to protect the internal network devices from denial-of-service-attacks.

Additionally, Out-of-dialog SIP requests can be filtered based on the source and target call number or prefixes defined by the administrator.

Media streams are only allowed after a session was initiated using SIP. Malformed packets are always refused or dropped.

The TOE also contains a mechanism to send syslog messages to a dedicated syslog server outside of the TOE in the management network. The secure storing of these messages is performed by the syslog server, whereas the sending of the syslog messages is part of the TOE.

1.2.2. Management

The following systems are in the management network and are needed for the management and configuration of the TOE. Not all systems are part of the TOE but part of the secunet SBC product. The ABC Monitor, dedicated Syslog server and operator workstation are part of the management network which is physically separated from the internal and external network (see Figure 1 below).

JSON Configuration interface

The TOE is configured by using configuration files in the JSON format, a standardized platform-independent text file format. These configuration files are deployed on the TOE by "pushing" them directly onto the TOE with an established SSH session.

All users that log in on the SBC Container ("TOE Administrator") must be members of the Linux group "sudoers" which allows them to create, delete and modify filtering options used to enforce the SIP Information Flow SFP. Every TOE Administrator needs to be authenticated by the TOE or by an external LDAP server located in the management network.

During the deployment of the configuration files, the SBC Container directly uses SSH, and the access control mechanism is performed by the built-in Linux access control mechanism. This means, that the configuration files are only deployed in specific locations based on the file systems permissions.

The TOE shall provide the following management functions:

1. Filter Configuration

   Authorized Administrators shall be able to

   - create, modify, and delete the signaling (SIP) and media stream endpoints on the SBC Container,
   - create, modify, and delete the routing of SIP calls, SIP registrations and other SIP messages between the realms and elements in the network,
   - create, modify, and delete the rules for filtering and manipulation options of SIP calls, SIP registrations and other SIP messages,
   - create, modify, and delete the rules for filtering and manipulation options of media stream packets and
   - manage all *SIP Information Flow SFP* security attributes.

2. User Management

   The secunet SBC Container shall also provide the functionality to modify the user accounts. If local authentication is used, the SBC Container also assures that at least 8 characters are used as user passwords when using local authentication.

ABC Monitor (not part of the TOE)

The ABC Monitor is the centralized monitoring system for the SBC application which allows administrators to assess the status of one or more SBCs, e.g., the number of currently open calls or the information on blocked communication attempts. It consists of a configuration database, a web GUI for the management of this database as well as different interfaces used for failure detection and analysis.

Dedicated Syslog Server (not part of the TOE)

Recording of the secunet SBC Container syslog messages is not performed by the TOE, but by a dedicated syslog server in the same network segment, i.e., the management network. This allows the ABC monitor to focus on its main tasks and provides a better scalability. The server may be a Linux system with a Syslog-NG service. Additionally specific messages can be sent to a further central syslog of the network management.

Operator workstation (not part of the TOE)

The operator workstations are also located in the management network, separated from the internal and external network. Access to the ABC Monitor and the SBC Container SSH interface is only possible from the management network and can additionally be secured by using an encrypted connection (https or SSH).

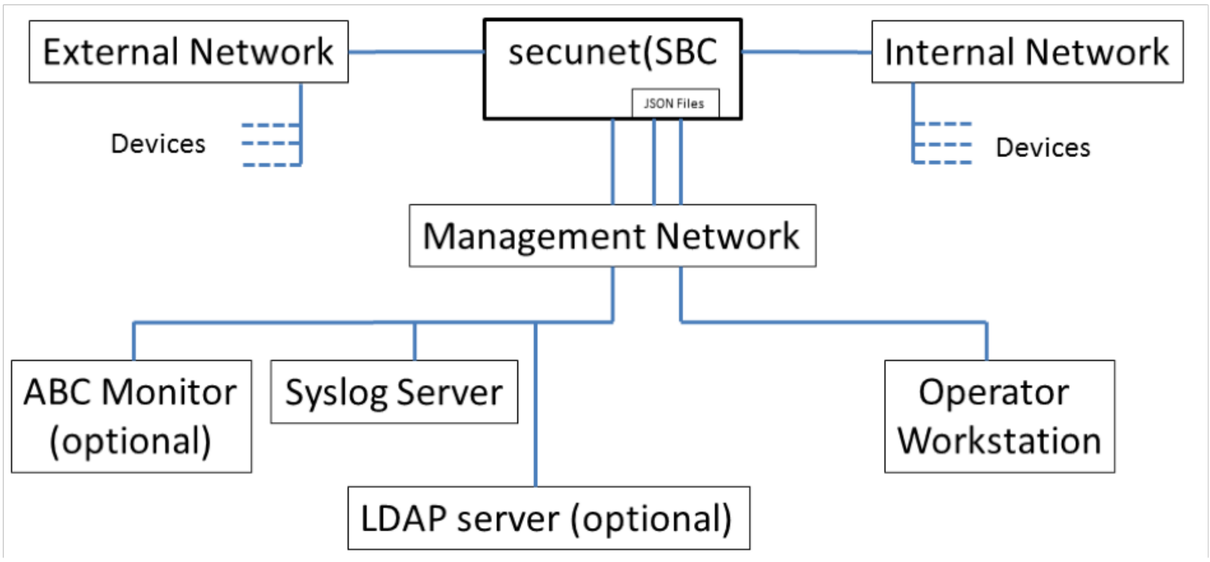

Figure 1 secunet SBC network topology

1.3. TOE Description

1.3.1. Physical Scope

The secunet SBC Container is a software product running in a Linux container environment. The used container environment is *systemd-nspawn*. This container technology allows the administrator of the underlying operating system to easily install and update the secunet SBC Container.

All parts of the TOE delivery are listed in the following table:

TOE part	Version	file name and SHA-256 hash
secunet SBC Container (software)	4.2.10-16	secunet-sbc-container-4-2-10-16.tgz SHA256: 430b3772ab272eab40dbdee530b51e6271aa1db1b1e01a7b38a8fba688e977d8
Secunet SBC Container Handbook 4.2 documentation	2.2	SBC – AGD v2.2.pdf SHA256: 63f013ad5a7d043b135c6e70bff6d4af25b52d8ed5cc9ee056b0ee137c75dd22

Table 1 Scope of the TOE delivery

1.3.2. Logical Scope

The TOE itself is a part of the secunet SBC Container software running in a Linux container environment. Figure 2 below shows the main components of the TOE as well as the TOE environment. The data flow between the management network and the SBC as well as the data flow between the internal and external network are depicted as a blue line to show how the data "travels" through the underlying OS including the packet filtering (IPtables) module to the SBC:

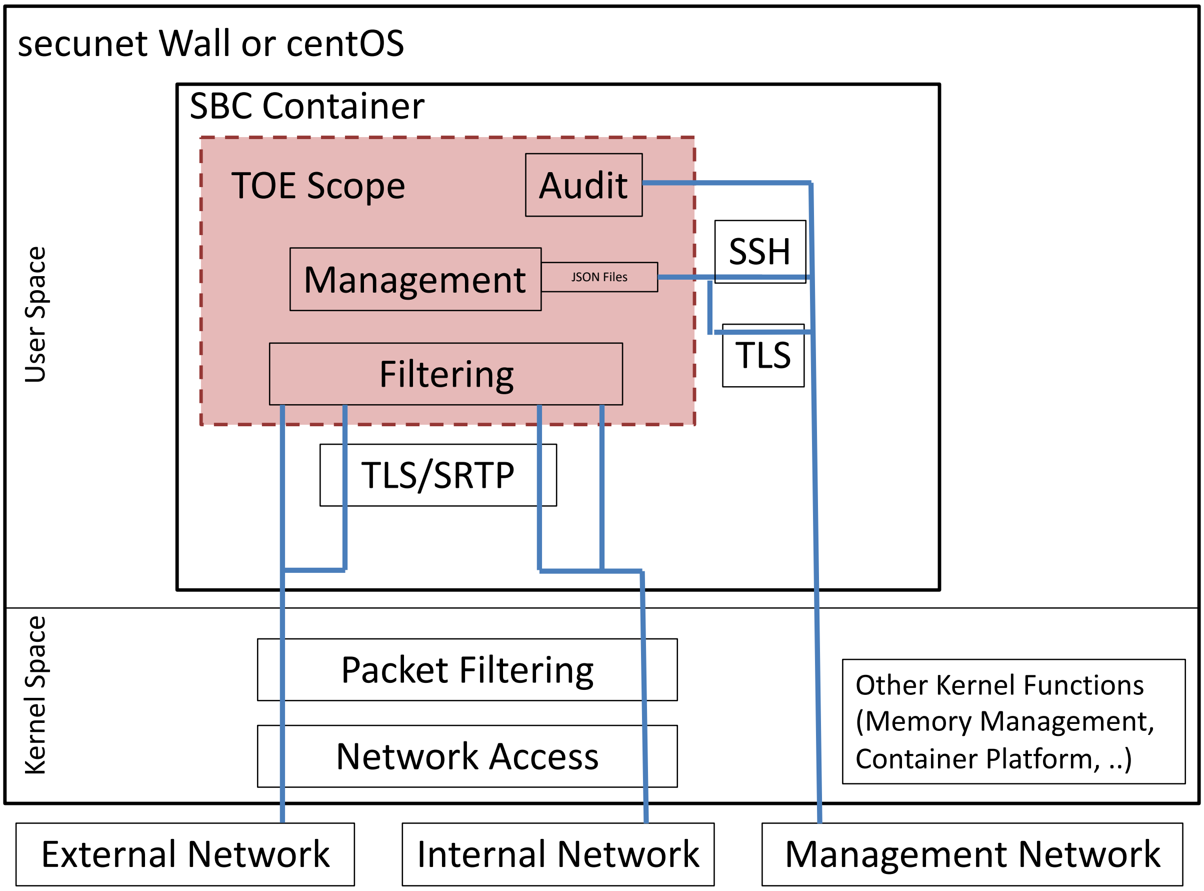

Figure 2: Logical TOE Scope

The secunet SBC Container is the execution platform for the TOE. It is integrated in a Linux operating system platform as secunet Wall at least version 6.1.0 or a hardened centOS at least version 7.9. The TOE includes all needed libraries to enable its basic functionality. This includes the following:

Filtering

The main functionality of the TOE is the filtering and manipulation of SIP and media stream data packets. This serves two purposes: The packet headers from the inner network to the outer network are stripped from information which potentially could allow the attacker to determine the components used in the inner network, e.g. the user-agent field. Also, the header fields of packets from the external to the internal network are stripped in order to prevent exploitation of the internal components with malformed packets. The packets are filtered and processed on several protocol levels. A more detailed description is given in chapter 6.1.1.

Management

Further TOE functionality is the Management of its security functionality. The TOE provides a JSON interface which allows administrators to update the TOE filtering policies and other security relevant TOE functions such as user and access control management by creating the JSON configuration files and deploying them on the TOE over an SSH connection. The TOE enforces an authentication of the administrators by using the internal database of the Linux authentication mechanism or an external LDAP service.

Audit

The TOE sends syslog messages to a dedicated syslog server in the management network. The sending of the syslog messages is included in the TOE functionality whereas the receiving syslog server is part of the environment. See also 6.1.4.

Guidance Documentation

The Guidance documentation comprises the SBC Handbook and guidance documentation on how to set up and operate the TOE according to the certified configuration.

The following functionality is not in the TOE scope:

Protocol handling incl. cryptography

The following two protocols are used which provide the confidentiality and integrity of the transferred data.

1. TLS can be used to protect the communication packets between the SBC and the endpoint (internal or external network). Additionally, the communication between the TOE and the ABC Monitor (Monitoring Server) and Operator workstation in the management network is protected by TLS. This TLS implementation contains all the protocol handling and the cryptographic implementations of various algorithms.
2. SRTP can be used to protect communication packets between the SBC and the communication endpoint in the internal or external networks.

Both protocols ensure the confidentiality and integrity of the transferred data. They are not part of the TOE functionality. However, to ensure that they do not contain any unwanted attack surface they are assessed during the vulnerability analysis of the evaluation.

1.3.3. TOE Type

The TOE Type is a Session Border Controller software. A Session Border Controller (SBC) is a device which is deployed in Voice-over-IP (VoIP) networks to manage the signaling and media streams of audio and video communication. The hardware device and operating software which serves as the platform of the TOE is a hardened Linux system, secunet Wall at least version 6.1.0 or a hardened centOS at least version 7.9. This system may also perform additional tasks such as packet filtering and routing on TCP and UDP level. In any case the SIP and media stream packets shall be passed to the TOE which performs further packet filtering and manipulation of these packets.

1.3.4. Required Non-TOE hardware/software/firmware

As a software-only TOE the secunet SBC Container needs a Linux operating system with the *systemd-nspawn* container management technology installed. The Linux OS needs a network packet routing functionality to send the VoIP packets to the SBC.

The hardware is under full control of the operating system. However, the connected networks have to be separated physically, especially the management network, to allow the SBC to perform the intended operation correctly.

2. Conformance Claim

2.1. Common Criteria Conformance Claim

This Security Target claims conformance with Part 2 ([2]) and part 3 ([3]) of the Common Criteria 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 and AVA_VAN.5.

ALC_FLR.2 adds flaw remediation procedures.

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 **organizational security policies** the TOE has to comply to.

3.1. Assets

The following assets are defined

3.1.1. Management Interface User credentials

If local authentication is used the username and password hash of each TOE administrator is stored inside the TOE and shall be protected to ensure that only authorized users can use these credentials to access the TOE´s management interface.

3.1.2. Information about the internal network

The network structure, used components, protocols and services of the internal network shall be protected from disclosure to non-administrators in order to avoid attacks against this network.

3.1.3. Configuration data

The filtering rules which define the filtering policy and all other relevant configuration data must be kept integrity protected.

3.1.4. Resources of the internal network

This asset covers the functionality of the components in the internal network. It must be ensured, that the components can perform their defined operations without interference.

3.2. Subjects

3.2.1. System Administrator

The System Administrator is responsible for the secure setup and operation of the Linux operating system which acts as the TOE platform and the environment such as the management network including the syslog server. The System Administrator also installs the TOE on the Linux operating system and is responsible for TOE updates, i.e. by replacing the container with the newer version.

3.2.2. TOE Administrator

The TOE Administrator group contains all users who can login at the TOE. All TOE Administrators are members of the “sudoers” group. Authentication is either performed locally or by the external LDAP server. The authenticated users can access the filtering management functions and can create, delete, and modify filtering rules.

3.2.3. SIP user

All subjects in the internal or external network which use the SIP connections of the TOE fall under this role.

3.3. Assumptions

3.3.1. A.PhysicalProtection

It is assumed that the server on which the TOE together with the underlying operating system platform is running, is located in a secured environment which does not allow an attacker to get any physical access. This also holds for the Management network including all servers and the machine from where the user connects to the TOE.

3.3.2. A.ManagementNetwork

It is assumed that the access to the management interface is only possible from a distinct and secure management network which is physically separated from both the internal and external network and only accessible by administrators. Also, the machine used by the Administrators to connect to the SSH interface, the optional LDAP server, the SNMP protocol, the optional ABC Monitor and the server(-s) which receive and store the audit logs from the TOE are located in this secure management network. When using the LDAP server, this server must implement the LDAP protocol correctly. Also, no data from the LADP authentication shall leave the secured management network.

3.3.3. A.Administrators

It is assumed that the administrators of the TOE and the underlying operating system platform are well skilled and trustworthy, follow the guidance and configure as well as operate TOE and operating system platform in a secure way. It is also assumed that the TOE Administrator is an expert in the field of VoIP technology and the setup and management of a Session Border Controller.

3.3.4. A.NetworkFlow

It is assumed that the hardware machine running the TOE operating system platform provides the only connection between the internal and the external network and that the operating system platform is configured that way that all VoIP traffic passes the TOE.

3.4. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the TOE method of use in the operational environment and the assets stored in or protected by the TOE. The TOE in collaboration with its IT environment shall avert the threats as specified below.

The threat agent for all threats is an attacker who an attack potential “high” who is located in the external network and is able to send arbitrary data to the TOE.

3.4.1. T.Bypass

An attacker from the external network tries to bypass the security functions of the TOE in order to gain unauthorized access to resources in the protected networks, e.g. by sending IP packets to circumvent filters. This can include (but is not limited to):

- An attacker tries to call a restricted call number
- An attacker tries to use a not allowed codec
- An attacker tries to send a message which is not valid SIP
- An attacker tries to send RTP packets without an active SIP session.
- An attacker tries to send RTP packets which exceed the bandwidth negotiated for this session

This bypassing allows the attacker to exploit vulnerabilities of devices in the internal network.

3.4.2. T.InformationLeakage

An attacker from the external network gets insights into the internal network which could provide useful information to mount further attacks. This useful information includes IP addresses of internal network elements, vendor- or device-specific information stored in the header fields or other information which could be extracted from the packets, e.g. specific header-extensions.

3.4.3. T.DenialOfService

An attacker sends more SIP requests from the external to the internal network than the internal devices can handle. The resources in the internal network then become inaccessible due to the overload.

3.4.4. T.UserDataLeakage

An attacker from the external or internal network compromises confidential user data stored on the TOE, e.g. credentials used for the SSH authentication.

3.4.5. T.UnauthorizedAccess

An attacker may try to access restricted TOE functions such as changes of filtering configuration.

3.4.6. T.Unaccountability

An attacker leaves no traces and therefore the attack remains undiscovered.

3.5. Organisational Security Policies

3.5.1. Organisation Security Policies for the Operation Environment of the TOE

The following OSP is to be enforced by the TOEs operational environment:

OSP.SecurePlatform

The TOE software must be deployed on a hardened Linux Operating System defined in chapter 1.3.2. The container functionality *systemd-nspawn* must be provided by the platform. It must also ensure that the integrity of the TOE is protected against malicious manipulation. The operating system administrator must make sure that the operating system is installed and operated in a secure way.

3.5.2. Organisation Security Policies for the TOE

The following OSP is to be enforced by the TOE:

OSP.Managment

The TOE shall allow authenticated administrators to modify the filtering policies of the TOE.

4. 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 (in Chapter 4.3).

4.1. Security Objectives for the TOE

4.1.1. O.SecureProtocol

The TOE performs data inspection and filtering of SIP and media stream packets (media payload excluded) in accordance with a defined ruleset. This serves two purposes: It prevents IP addresses of the inner network from being exposed to the outside and also blocks malformed packets from the outer network. The total number of out-of-dialog-SIP-requests (for example: INVITE, REGISTER, SUBSCRIBE) per time period is limited so that the internal network effectively is prevented.

4.1.2. O.Audit

The TOE shall provide log messages for all management operations such as user creation or the setup of filtering rules to provide reliable audit logs and also provide accountability for the performed operations.

4.1.3. O.Authentication

The TOE shall provide a secure authentication mechanism to users with the role TOE Administrator.

4.1.4. O.Management

The TOE shall provide authenticated users the ability to access and change the packet filtering configuration.

4.2. Security Objectives for the Operational Environment

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

4.2.1. OE.SecurePlatform

The TOE software shall be deployed on a hardened Linux Operating System as defined in chapter 1.3.2. The container functionality *systemd-nspawn* has to be provided. It shall also ensure that the integrity of the TOE is protected against malicious manipulation. The operating system platform shall ensure that only packets from the internal and external networks with a destination port number that correspond to a signaling or media interface configured in the Secunet SBC Container are directed to the Secunet SBC Container. The signaling ports are the SIP and SIP/TLS ports defined in the signaling interface; The media ports are the port number corresponding to the port range defined in the media interface starting at 10000 minimum, as no other services are bound to any port equal or above 10000. Other packets received on these interfaces shall be dropped. The operating system platform shall ensure that from the internal and external network all SIP and media stream packets and no other packets are directed to the TOE. Other connections are only allowed from the secured management network over a dedicated and physically separated network interface. This includes SSH access for management purpose, LDAP authentication as well as monitoring (SNMP and monitoring access). The operating system platform shall further ensure that DNS requests are only allowed to be sent to the secured administrative network and DNS replies are only allowed from secured administrative network. The operating system Administrator has to make sure that the operating system is installed and operated in a secure way. The platform must also ensure that the configuration data which contains the filtering policy is kept integrity protected. Additionally, the platform must provide reliable time stamps to the TOE in order to allow the TOE to provide reliable audit records.

4.2.2. OE.PhysicalAccess

The TOE shall be used in a controlled environment. The environment shall ensure that only authorized personnel can access the TOE physically. This also holds for the Management network including all servers and the machine from where the user connects to the TOE.

4.2.3. OE.ManagementNetwork

Access to the SSH interface shall only be possible from a distinct and secure management network which shall be physically separated from both the internal and external network and only accessible by administrators. Also, the machine used by the TOE Administrator to connect to the SSH interface, the optional ABC Monitor, the SNMP protocol, and the server(-s) which receive and store the audit logs from the TOE shall be located in this management network. If LDAP authentication is configured, no data transferred during the authentication shall leave the secured management network.

4.2.4. OE.Administrators

The administrators of the TOE and the underlying Linux operating system shall be well skilled and trustworthy and shall configure as well as operate TOE and operating system platform in a secure way. The TOE Administrator shall be an expert in the field of VoIP technology and the setup and management of a Session Border Controller.

4.2.5. OE.NetworkFlow

The hardware machine running the TOE and the Linux operating system platform shall be deployed so that it provides the only connection between the internal and the external network. The operating system platform shall be configured that signaling and media traffic from internal and external network handed is over to the Secunet SBC Container and other packets received on these interfaces are dropped. Additionally, the internal and external networks must be connected to physically separated network interfaces (no VLANs or similar mechanisms).

4.2.6. OE.LDAP

If user authentication is performed by a remote LDAP server, the LDAP server shall be located in the secure management network. The LDAP server shall ensure that no data transferred during authentication leaves the management network. The LDAP server also needs to provide a mechanism to limit the authentication attempts, when using LDAP authentication. This server also needs to implement the LDAP protocol correctly.

4.2.7. OE.Syslog

Syslog messages are generated by the TOE and sent to the syslog server in the management network. This syslog server shall provide a secure storing mechanism to ensure that the integrity of the received syslog messages is protected after the syslog server receives the message.

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.SecurePlatform	OE.PhysicalAccess	OE.ManagementNetwork	OE.Administrators	OE.NetworkFlow	OE.LDAP	OE.Syslog	O.SecureProtocol	O.Audit	O.Authentication	O.Management
OSP.SecurePlatform	X										
OSP.Managment											X
A.PhysicalProtection		X									
A.ManagementNetwork			X								
A.Administrators				X							
A.NetworkFlow					X						
T.Bypass	X				X			X			
T.InformationLeakage	X				X			X			
T.DenialOfService								X			
T.UserDataLeakage	X							X			
T.Unaccountability							X		X		
T.UnauthorizedAccess			X			X				X	

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.SecurePlatform, OE.NetworkFlow and O.SecureProtocol*. The environmental objective *OE.NetworkFlow* ensures that all network traffic is routed over the underlying Linux operating system. The environmental objective *OE.SecurePlatform* ensures that packets on a lower protocol level are filtered by the environment. By *OE.NetworkFlow* it is ensured that all data on the SIP protocol level is directed to the TOE. The TOE itself filters and transforms the packets implementing the objective *O.SecureProtocol*.

The threat **T.InformationLeakage** describes that an attacker gains information about the internal network topology, organization, protocols, services, and devices. This information leakage is countered by a combination of the objectives *OE.SecurePlatform, OE.NetworkFlow and O.SecureProtocol*. The environmental objective *OE.NetworkFlow* ensures that all network traffic is routed over the underlying Linux operating system. The environmental objective *OE.SecurePlatform* ensures that packets on a lower protocol level are filtered by the environment. By *OE.NetworkFlow* it is ensured that all data on the SIP protocol level is directed to the TOE. The TOE itself transforms all passing packets implementing the objective *O.SecureProtocol*, so that all sensitive information is stripped from the packets.

The threat **T.DenialOfService** describes that an attacker tries to flood the system with packets that cause the systems of the internal network to become inaccessible due the high load. It is countered by *O.SecureProtocol* which ensures that defined functionality can only be performed from the local network. Furthermore, the total number of out-of-dialog-SIP-requests (for example: INVITE, REGISTER, SUBSCRIBE) per time period is limited by this TOE security objective which prevents against Denial-of-Service attacks against the internal network effectively.

The threat **T.UserDataLeakage** describes that an attacker gains access to confidential data stored in the TOE. This threat is countered by a combination of the environment objective *OE.SecurePlatform* and the TOE objective *O.SecureProtocol*. The operating system platform shall protect the authenticity and integrity of the TOE which cannot be prevented by the TOE itself. The correct implemenmtation of the objective *O.SecureProtocol* ensures that no sensitive information can be accessed by an attacker by using the Protocol itself.

The threat **T.Unaccountability** describes that TOE users or attackers may not be accountable for the actions they conduct, thus allowing an attacker to escape detection. This threat is countered by *O.Audit*, which ensures that the log messages contain an identification of the TOE users that performs the operation. The log files are sent to the syslog server which shall handle and store the log files in a way that ensures their integrity. This is achieved by *OE.Syslog*.

The threat **T.UnauthorizedAccess** which describes that an attacker gets unauthorized access to the TOE is countered by the environmental objective *OE.ManagementNetwork* and the TOE objective *O.Authentication*. *OE.ManagementNetwork* ensures that access to the TOE management interface is only allowed from a dedicated Management Network. *O.Authentication* ensures that the TOE shall uniquely identify and authenticate the identity of all TOE users, before granting an administrator access to TOE management functions. *OE.LDAP* ensures that no data which could allow an attacker to get unauthorized access leaves the management network.

4.3.2. Covering the Organizational Security Policies

1 The organizational security policy **OSP.SecurePlatform**

is covered by OE.SecurePlatform as directly follows.

The organizational security policy **OSP.Managment** is covered by *O.Management* as directly follows.

4.3.3. Covering the Assumptions

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

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

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

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

5. Security Requirements

5.1. Security Functional Policies

The TOE shall implement the information flow control policy *SIP Information Flow SFP* defined as follows:

Subjects:

- Communication partners in the internal network
- Communication partners in the external network
- TOE

Security attributes for subjects:

none

Information (objects):

- IPs and ports in the internal network
- SIP Dialog Identifiers (Call-ID, From-tag, To-tag)
- Route, Record-Route and Via (IP addresses and ports that the SIP message has traversed in the internal network)
- IPs, SIP Dialog Identifiers and Route/Record-Route/Via headers
- Source call number
- Target call number

Security attributes for information (objects):

- List of allowed source call numbers or prefixes
- List of allowed target call numbers or prefixes
- Maximum value of INVITE requests / calls per time interval
- Maximum value of REGISTER requests / registrations per time interval
- Maximum value of SUBSCRIBE requests / subscriptions per time interval
- List of allowed SIP methods (e.g. INVITE, REGISTER, SUBSCRIBE, MESSAGE, REFER)
- Allowed headers (e.g. User-Agent, P-Asserted-Identity)
- Allowed Content-Types (e.g. application/sdp, application/pidf+xml)
- Allowed media types (e.g. audio, video)
- Allowed Codecs (e.g. G.711, G.729)
- Allowed SDP attributes (e.g. ptime, maxptime)

Operations:

- Transfer of information (This does not include routing)
- Call establishment using an INVITE request.
- Registration using a REGISTER request.

- Subscription using a SUBSCRIBE message

Rules:

- If configured, the TOE does not transfer internal IPs addresses to the external network.
- The TOE shall not transfer SIP Dialog Identifiers and Route/Record-Route/Via headers used in the internal network from internal to the external network.
- The TOE shall only transfer packets from the external network to the internal network which were analyzed and modified by the TOE.
- If configured, the TOE limits the number of calls per time interval from external communication partners to the Maximum value of calls per time interval.
- If configured, the TOE limits the number of registrations requests per time interval from external communication partners to the Maximum value of registrations per time interval.
- If configured, the TOE limits the number of subscriptions requests per time interval from external communication partners to the Maximum value of open subscriptions per time interval.
- The TOE shall only allow a media stream connection between participants after a SIP connection establishment has been performed. After the call has ended the media stream connection shall be closed.
- If configured, all requests are to be only allowed to pass the TOE if the source and target call number or prefixes appear in the corresponding list of allowed source or target numbers or prefixes.

5.2. Security Functional Requirements for the TOE

This chapter contains a description of each component and any related dependencies.

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.

5.2.1. Security Functional Requirements (SFRs) for the User Management

This chapter describes the SFRs for the user management provided by the TOE.

The TOE only maintains the role TOE Administrator. This role however is assigned to every user who is in the Linux group “sudoers” which allows the user to update TOE configuration.

5.2.1.1. FPT_TDC.1 Inter-TSF basic TSF data consistency

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [*the user role*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [*the user groups assigned to the user role*] when interpreting the TSF data from another trusted IT product.

5.2.1.2. FMT_SMF.1/User Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/User The TSF shall be capable of performing the following management functions: [

- *Authentication management: configuration of authentication measure (local or LDAP authentication)*

].

5.2.1.3. FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1 The TSF shall maintain the roles [TOE Administrator*, SIP communication partner*].

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

5.2.1.4. FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 The TSF shall restrict the ability to [modify] the [*password*] to [*TOE Administrator*].

5.2.2. Other Security Functional Requirements

These SFRs cover the remaining security functional requirements of the TOE.

5.2.2.1. FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*Other specifically defined auditable events*

- *blocked communication attempts*
- *changes of the configuration*
- *user login and logout*
- *unsuccessful login attempts*

]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*none*]

Application Note: *The TOE itself does not store log records. This is done by an external syslog server (see* OE.Syslog*). Reliable Time stamps, as required by this SFR are provided by the underlying operating system (see* OE.SecurePlatform*)*

5.2.2.2. FDP_IFC.1 Subset information flow control

Hierarchical to: No other components

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the [*SIP Information Flow SFP*] on [*all SIP users*].

5.2.2.3. FDP_IFF.1 Simple security attributes

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialization

FDP_IFF.1.1 The TSF shall enforce the [*SIP Information Flow SFP*] based on the following types of subject and information security attributes: [*types of subject and information security attributes defined in SIP Information Flow SFP*].

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: [*rules defined in SIP Information Flow SFP*].

FDP_IFF.1.3 The TSF shall enforce the [*SIP Information Flow SFP*].

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: [*none*]

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*none*]

.

5.2.2.4. FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [3] of unsuccessful authentication attempts occur related to [unsuccessful local authentication events since the last successful local authentication].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*disable the corresponding account for an administrator-configurable timeframe*].

5.2.2.5. FIA_SOS.1 Verification of secrets

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [*a minimum of 8 characters*].

5.2.2.6. FIA_UAU.1 Timing of authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*the SIP connection establishment and media stream data flow*] on behalf of the user to be performed before the user is authenticated.

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.

5.2.2.7. FIA_UID.1 Timing of identification

Hierarchical to: No other components

Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*the SIP connection establishment and media stream data flow*] 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.

5.2.2.8. FMT_MOF.1 Management of security functions behavior

Hierarchical to: No other components

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management functions

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behavior of] the functions [

- *Authentication management: configuration of authentication measure (local or LDAP authentication)*]

to [*TOE Administrator*].

5.2.2.9. FMT_MSA.1 Management of security attributes

Hierarchical to: No other components

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management

FMT_MSA.1.1 The TSF shall enforce the [*SIP Information Flow SFP*] to restrict the ability to [modify] the security attributes [*security attributes defined in SIP Information Flow SFP*] to [*TOE Administrator*].

5.2.2.10. FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*SIP Information Flow SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow [*no one*] to specify alternative initial values to override the default values when an object or information is created.

Note: Specification of alternative initial values is not supported by the TOE.

5.2.2.11. FMT_SMF.1/Filter Specification of management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1/Filter The TSF shall be capable of performing the following management functions: [

- *create, modify, and delete the signaling (SIP) and media stream endpoints on the SBC*
- *create, modify, and delete the routing of SIP calls, SIP registrations and other SIP messages between the realms and elements in the network*
- *create, modify, and delete the rules for filtering and manipulation options of SIP calls, SIP registrations and other SIP messages*
- *create, modify, and delete the rules for filtering and manipulation options of media stream packets*
- *Management of all SIP Information Flow SFP security attributes*].

5.2.2.12. FTA_SSL.3 TSF-initiated termination

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTA_SSL.3.1	The TSF shall terminate an interactive session after a [*configurable time interval of administrator inactivity at the SSH interface*].

5.3. Security Assurance Requirements for the TOE

The following table lists the chosen evaluation assurance components for the TOE. All assurance requirements for the evaluation of the TOE and its development and operating environment are those taken from the Evaluation Assurance Level EAL4.

Two augmentations were added:

- AVA_VAN.5 (Advanced methodical vulnerability analysis)
- ALC_FLR.2 (Flaw reporting procedures)

The augmentation AVA_VAN.5 was chosen because it adds the attack potential “High”. The augmentation ALC_FLR.2 was chosen because it adds procedures for accepting and acting upon reports of security flaws.

Assurance Class	**Assurance Components**	
ASE	ASE_INT.1	ST introduction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
ADV	ADV_ARC.1	Security architecture description
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD	AGD_OPE.1	Operational user guidance

	AGD_PRE.1	Preparative procedures
ALC	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	**Flaw reporting procedures**
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ATE	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA	**AVA_VAN.5**	**Advanced methodical vulnerability analysis**

Table 2: SAR requirements

5.4. Security Requirements Rationale

5.4.1. TOE Functional Requirements Rationale

TOE Security Functionality	**SFR ID**	**O.SecureProtocol**	**O.Management**	**O.Audit**	**O.Authentication**
Security Audit	FAU_GEN.1			X	
User Data Protection	FDP_IFC.1	X			
	FDP_IFF.1	X			
Identification and Authentication	FIA_AFL.1				
	FIA_SOS.1		X		
	FIA_UAU.1				X
	FIA_UID.1				X
Security Management	FMT_MOF.1		X		
	FMT_MSA.1		X		
	FMT_MSA.3		X		
	FMT_MTD.1		X		
	FMT_SMF.1/User		X		
	FMT_SMF.1/Filter		X		
	FMT_SMR.1				X
	FPT_TDC.1				X
TOE access	FTA_SSL.3				X

Table 3: Coverage of Security Objectives by SFRs

The security objective **O.Audit** is met by FAU_GEN.1 FAU_GEN.1 describes which audit records are logged. This is completely fulfilled by the objective O.Audit.

The security objective **O.SecureProtocol** is met by FDP_IFC.1 and FDP_IFF.1. Both SFRs cover the *SIP Information Flow SFP*. The security objective O.SecureProtocol covers the protocol manipulation to enforce this SFP.

The security objective **O.Authentication** is met by FIA_AFL.1, FIA_UAU.1, FIA_UID.1, FMT_SMR.1 FPT_TDC.1, and FTA_SSL.3.

FIA_UID.1 and FIA_UAU.1 cover the Timing of identification and authentication. The objective O.Authentication ensures that user with the role TOE Administrator need to be identified and authenticated before they can perform any security related action on their behalf.

If authentication is performed locally, FIA_AFL.1 limits the authentication attempts. If authentication via LDAP is used, the SFR FPT_TDC.1 ensures that the data from the LDAP server is interpreted correctly. In both cases (local or remote authentication Users are assigned roles (FMT_SMR.1).

After a configurable time interval the session is closed automatically (FTA_SSL.3).

The security objective **O.Management** covers all aspects related to the management of users and the filtering policy.

The access restrictions enforced by the TOA are ensured by the SFRS FMT_MOF.1, FMT_MSA.1, FMT_MSA.3 and FMT_MTD.1.

The specifications of the management functions restricted to the user TOE Administrator are defined by the SFRs FMT_SMF.1/User and FMT_SMF.1/Filter

When new users are created the SFR FIA_SOS.1 ensures that a minimum password length is enforced by the TOE.

5.4.2. Fulfilling of Dependencies

5.4.2.1. Fulfilling of Security Functional Requirements Dependencies

The following table shows that all dependencies are met:

SFR	Dependencies	Fulfilled by
FAU_GEN.1	FPT_STM.1	Dependency is not fulfilled because the provision of reliable time stamps is performed by the TOE environment.
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_SOS.1	No dependencies	-
FIA_UAU.1	FIA_UID.1	FIA_UID.1

FIA_UID.1	No dependencies	-
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/User
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_IFC.1 FMT_SMR.1 FMT_SMF.1/Filter
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1/User
FMT_SMF.1/User	No dependencies	-
FMT_SMF.1/Filter	No dependencies	-
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_TDC.1	No dependencies	-
FTA_SSL.3	No dependencies	-

Table 4: Fulfilling of SFR dependencies

5.4.2.2. Fulfilling of Security Assurance Requirements

A complete EAL level was chosen (EAL4) and then augmented. The EAL level itself is consistent and fulfils all dependencies. The dependencies which are added by the augmentation are also fulfilled, see table below:

Augmen-tation	Dependencies	Rating	Fulfilment of dependencies
AVA_VAN.5	ADV_ARC.1	is part of EAL4	Dependency fulfilled

Augmen-tation	Dependencies	Rating	Fulfilment of dependencies
	ADV_TDS.3	is part of EAL4	Dependency fulfilled
	ADV_FSP.4	is part of EAL4	Dependency fulfilled
	ADV_IMP.1	is part of EAL4	Dependency fulfilled
	AGD_OPE.1	is part of EAL4	Dependency fulfilled
	AGD_PRE.1	is part of EAL4	Dependency fulfilled
	ATE_DPT.1	is part of EAL4	Dependency fulfilled
ALC_FLR.2	none	n/a	n/a

Table 5: Fulfilling of SAR dependencies

6. TOE Summary Specification

The TOE provides the following security functionality:

6.1. TOE Security Functionality

6.1.1. SF.PacketFiltering: Packet Filtering

The TOE performs an inspection and filtering on several levels:

SIP method filtering: the TOE performs filtering based on the SIP method, e.g.: “INVITE”, “SUBSCRIBE”, “REGISTER”, to allow e.g. only to register devices from the inside network. The TOE can also set a limit of invite messages per time interval from outside to protect the components in the inner network from Denial-of-Service (DoS) attacks. Another filtering method is the manipulation of the SIP header field. This serves two purposes: The packet headers from the inside network to the outside network is stripped from information which potentially could allow the attacker to determine the components used in the inside network, e.g. the user-agent field. Also, the header fields of packets from the external network to the internal network are stripped in order to prevent exploitation of the internal components with e.g. malformed SIP or media packets.

At the body of the message the content type is filtered to e.g. “application-sdp”, to allow only the correct content. Also, the media type can be set to e.g. audio, video or application. Finally, the codec can be filtered to allow only specific codecs, e.g. G.711 or Opus.

To hide the topology of the internal network the TOE implements a strict Back-to-Back user agent to establish two completely separated calls originating from the SBC. Thus, at the external network no internal dialog IDs (Call-ID header field, ’tag’ attribute in From and To header fields) and IP addresses are visible. The filtering of dialog IDs is always active “by design”, the filtering is always active. The filtering of internal IP addresses can be configured by the TOE administrator.

Media streams such as (S)RTP shall only be allowed if a session was initiated before using SIP. Malformed SIP and media stream packets shall always be refused or dropped.

This security function covers FDP_IFC.1 and FDP_IFF.1.

6.1.2. SF.Management: Management of Security Functions

The initial deployment as well as updates of the TOE are performed by changing the whole container using appropriate tools. This is out of the TOE scope and part of the TOE environment.

The TOE can be configured by using the JSON configuration files which is deployed directly on the SBC by using the SSH interface.

The TOE only maintains the role TOE Administrator. This role however is assigned to every user who is in the Linux group "sudoers" which allows the user to update TOE configuration. The TOE allows the user with the role TOE Administrator to define complex filtering and protocol management rules. This includes:

- create, modify, and delete the signaling (SIP) and media stream endpoints on the SBC,
- create, modify, and delete the routing of SIP calls, SIP registrations and other SIP messages between the realms and elements in the network,
- create, modify, and delete the rules for filtering and manipulation options of SIP calls, SIP registrations and other SIP messages,
- create, modify, and delete the rules for filtering and manipulation options of media stream packets and
- manage all *SIP Information Flow SFP* security attributes.

This Security function covers FMT_SMF.1/User, FMT_MTD.1, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1/Filter and FMT_SMR.1.

6.1.3. SF.Authentication: Authentication of Administrators

Users can log in at the management interface with username and password. The Authentication is performed either locally or by using an external LDAP server, depending on the TOE configuration. If Authentication is performed locally the password needs a minimum size of 8 characters. After three wrong authentication attempts the user account is disabled for a configurable time period to prevent brute force attacks against the management interface.

When external authentication is used the authentication of the user is performed by the LDAP server. Then after a successful authentication at the LDAP server the TOE assigns the access conditions of this user based on the roles assigned to the user in on the LDAP server.

This Security function covers FPT_TDC.1, FIA_AFL.1, FIA_SOS.1, FIA_UID.1, FIA_UAU.1 and FTA_SSL.3.

6.1.4. SF.Logging: Security Logging

The TOE provides several interfaces for logging and analyzing of the VoIP network.

A syslog daemon is running on the TOE which writes log files to a configured remote syslog server located in the management network. Additionally, the TOE sends event messages to a database in the management network, which can then be reviewed by the ABC Monitor.

This Security function covers FAU_GEN.1.

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

SFR	TOE Security Functionality			
	SF.PacketFiltering	SF.Management	SF.Authentication	SF.Logging
FPT_TDC.1			X	
FMT_SMF.1/User		X		
FMT_MTD.1		X		
FAU_GEN.1				X
FDP_IFC.1	X			
FDP_IFF.1	X			
FIA_AFL.1			X	
FIA_SOS.1			X	
FIA_UAU.1			X	
FIA_UID.1			X	
FMT_MOF.1		X		
FMT_MSA.1		X		
FMT_MSA.3		X		
FMT_SMF.1/Filter		X		
FMT_SMR.1		X		
FTA_SSL.3			X	

6.3. Self-Protection against Interference and Logical Tampering

The TOE provides several self-protection mechanisms that protect the TOE from interface and logical tampering:

Container Runtime

The container runtime described in the security architecture [ARC] provides self-protection for the Secunet SBC container.

Integrity Protection

The TOE contains a signed list of checksums for all the binaries and configuration file templates that enabled the TOE administrator to check the integrity of the TOE before starting it. During the start procedure, the relevant configuration files are re-generated to assure that correspond to the templates.

Configuration Checking

The TOE checks any new JSON configuration file before activation on the configuration interface.

Network packet checking

Within the Signaling and Media processing Subsystem, the packets received over the socket API are checked properly to avoid buffer overflows and invalid syntax. In particular, the lengths of the packets that can be received are limited, and bigger packets are dropped or refused directly by the transport layer.

The signaling interface is further secured by strict string boundary checking in the first SIP parser layer which has been extensively fuzzy tested by an external contractor on 2 recent occasions.

Upper parser layers (used for example in the User Agent and B2BUA code) make use of the string class defined in the C++ Standard Template Library (STL) that throws exceptions when boundaries are crossed.

On the media interface, the sizes indicated in the RTP packet headers are checked for consistency and boundaries to avoid accessing memory locations outside of the packet buffer. These consistency checks have been as well fuzzy tested by an external contractor together with the SIP parser.

6.4. Self-Protection against Bypassing

The TOE protects itself against bypassing on all TSFIs in the following ways:

TSFI Network Traffic Interface

On the container host, IP forwarding is switched off (or forbidden through firewall rules), so that the only way for packets to traverse the TOE on the network traffic interface is to pass through the Signaling and Media Processing Subsystem.

As shown in the ADV_TDS document, network packets on that interface are retrieved from the kernel socket API and passed to the higher layers for further processing, including the rule engine configured with its set of rules. If a particular packet should not be blocked or refused, it is passed to the other side and forwarded. The TOE does not allow or enable any other way, nor does it allow any modification of the IP forwarding settings or firewall rules on the container host.

TSFI Configuration Interface

The configuration interface is only accessible from the administrative network interface and does not allow any access to it until the user is properly authenticated by the secure shell daemon (sshd). It uses the User Authentication Subsystem to verify the user's credentials and finally authenticate the user.

Local authentication is always enabled, as it is based on file system operations that needs no special initialization during container start. The container host implements through its kernel all the basic file system operations, which are ready to be used once the TOE is started.

JSON Interface

The JSON interface is used manually through the Configuration Interface when a configuration file is activated manually.

When a configuration file is activated manually with the appropriate command line utility, the rest of the chain of configuration activation cannot be bypassed based on a specific JSON file.

LDAP Interface

The LDAP interface is solely used to authenticate users while accessing the Configuration Interface through remote secure shell. It is not involved in other security function or interfaces and can thus not interact with them.

7. Glossary and Acronyms

Term	Definition
JSON	JavaScript Object Notation
RTP	Real-Time Transport Protocol
SSH	Secure Shell
SIP	Session Initiation Protocol
SRTP	RTP over TLS
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VoIP	Voice over IP

7.1. References

7.1.1. Criteria

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology (CEM), Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[5] Anwendungshinweise und Interpretationen zum Schema, AIS20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik

[6] Anwendungshinweise und Interpretationen zum Schema, AIS31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, Bundesamt für Sicherheit in der Informationstechnik