Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1116-V2-2022

for

secunet wall, Version 6.1.0

from

secunet Security Networks AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1116-V2-2022 (*)

Firewall

secunet wall, Version 6.1.0

from	secunet Security Networks AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2, AVA_VAN.5 und ASE_TSS.2

SOGIS
Recognition Agreement
for components up to
EAL 4

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 8 April 2022

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of SOGIS-MRA, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained some components that are not mutually recognised in accordance with the provisions of the SOGIS MRA. For mutual recognition the EAL 4 components of these assurance families are relevant.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product secunet wall, Version 6.1.0 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1116-2020.

The evaluation of the product secunet wall, Version 6.1.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 4 April 2022. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: secunet Security Networks AG.

The product was developed by: secunet Security Networks AG.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 8 April 2022 is valid until 7 April 2027. Validity can be re-newed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product secunet wall, Version 6.1.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Deutschland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the secunet wall 6.1.0 which 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.

The secunet wall supports IPv4 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 integrated in a Linux operating system platform, where a Packet Filtering module is placed.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_FLR.2, AVA_VAN.5 und ASE_TSS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Details
SF1 Information Flow Protection	See ST [6], Chapter 6.1.1
SF2 Management	See ST [6], Chapter 6.1.2
SF3 Container Authentication	See ST [6], Chapter 6.1.3
SF4 Security Audit	See ST [6], Chapter 6.1.4

Table 1: TOE Security Functionalities

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

secunet wall, Version 6.1.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	Installationsmedium (USB stick) ISO-Hybrid-Image secunet wall Wirksystem 6.1.0.2 (Please note that secunet wall version 6.1.0.2 includes a patch, where the last digit represents a minor software change.) Including public signing key secuwall-gpg-public_signingkey.asc	Labelling “secunet-wall Wirksystem 6.1.0“ on installation medium “secunet wall 6.1.0.2” displayed on login screen	Physical Delivery
2	DOC	secunet wall Administrationshandbuch (Version 1.1) [8]	manual.pdf Date: 25.02.2022 SHA-512 Checksum: 7decf599f8ab0c001f9621f5d05410355f49cfd2c4bd611f6e5b5ad19ef48e395216cd156631b13a41cb20db040decf2a5bce930612061bc59776bc7686a4119	Installation medium
3	DOC	Release Notes [9]	release-notes.pdf Date: 25.02.2022 SHA-512 Checksum: 36536d5a585acb1447b90ebaa36006fa777cc7ce3e2019bcdb8591eb14f8f8431ab712c518fc554d27c8ff15efa739fbec60004ba8425f901c3f8fe19bef860e	Installation medium
4	SW	Signed checksum file	ISO-Hybrid-Image: bzImage.sig rootfs.squash.sig VERSION.sig all.sha512.asc	Installation medium

Table 2: Deliverables of the TOE

The TOE is delivered on an installation medium (USB stick) that is handed over to the consumer.

The items 2 to 4 in Table 2 are part of the delivery on the installation medium. They are part of the ISO-Hybrid-Image stored on the installation medium. The secunet wall

guidance [8] is also delivered on non-writable CD ROM. This copy of the Guidance documentation is binary identical to the original in the ISO-Hybrid-Image on the installation medium.

Remark on item 4 of the table above:

The Signed checksum file is a text file that contains a list of the delivered file names and binaries and their sha512 hash values. The whole file is enclosed in an open-PGP block that is signed with the secunet private key. This signature can be verified with the public key secuwall-gpg-public_signing-key.asc.

The binaries that comprise the TOE are:

- Release Linux Kernel, Identification: bzImage, SHA-512 hash value:
  a85385fce572766017062ce7294537df078625341a4c6fca0000e02787788950432d1fab21969cdbcd3b38722f10f9c061fa8faef75494c27dc5d7375cb20f64
- Release Userspace, Identification: rootfs.squash, SHA-512 hash value:
  7d54c0c3a9b10448985ee8b19af0d0c27781404116b39fa96f2404c73360ae223f3eb7947302fd41acda674e9e33faeffdc6dac635f382d35ba004fd71c93537
- Release Version, Identification: VERSION, SHA-512 hash value:
  e2968cb60a105016dd1ca014c0bfb1fd453c15d307c473a2d6a67ab4577c1b93b0eebf1d23b7efc304791a2b4d7e68b09108acdd3b7c8a9d965a846ad66a1bb8

The TOE can be uniquely identified by the SHA-512 checksums in the file all.sha512.asc which also contains a signature that can be verified with the public key in the file secuwall-gpg-public_signing-key.asc.

The TOE is delivered to the consumer on an installation medium (USB stick). Chapter 5.1 of the guidance [8] provides the administrator with information how to verify the authenticity of the TOE. The authenticity check is divided into two steps: first the administrator has to check the authenticity of the public PGP key secuwall-gpg-public_signing-key.asc delivered via installation medium. Therefore, the administrator has to check the validity against the checksum and has to call the support via telephone for the fingerprint of the public signing key. To perform the PGP operations a PGP implementation, e.g. the open source tool GnuPG, must be used. The delivered public key must be imported to calculate the fingerprint. If the fingerprint does not match the fingerprint from the project manager, the user must cancel the process and repeat the delivery process. Otherwise he can proceed to the second step: verification of the digital signature of the hash sum file all.sha512.asc. Therefore, the PGP tool must be used to verify the integrity of the hash sum file. If the hash sum file was signed with the correct key, the SHA512 sums of all files need to be calculated by using any tool that calculates the SHA-512 hash sum from a given file. Then the calculated hash sums must be compared to the ones listed in the file all.sha512.asc. If everything is correct the user must check whether the version numbers of secunet wall and guidance match version mentioned in the certification report. So the user can ensure that he has received the certified TOE.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the issues Information Flow Protection, Management, Container Authentication, and Security Audit.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The list of objectives which have to be met by the environment can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE is a firewall including packet filter functionality. The secunet wall comprises a 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. The secunet wall relies on information available at OSI layer 3 and layer 4 for policy enforcement. The functionality for packet filtering is part of the Linux operating system. The secunet wall supports IPv4 and IPv6 protocols. IPv6 is not part of the TOE. The secunet wall also supports LDAP. LDAP is not part of the TOE. This is an overview of the subsystems of the TOE and the corresponding TSF that were objects of the evaluation.

The security functions of the TOE are:

- SF1 Information Flow Control
- SF2 Management
- SF3 Container Authentication
- SF4 Security Audit

According to the TOE design specification these security functions are enforced by the following subsystems:

- TCP/IP Stack (represents the TSF SF1.1, SF1.2, SF1.3)
- TCP/IP Filter (represents the TSFs SF1.1, SF2.3, SF3.2, SF4.1 and SF4.2; supports the TSF SF2.2)
- Kernel-Log (supports the TSF SF4.1 and SF4.2)
- Kernel-Space Kommunikation (represents the TSF SF2.1; supports the TSF SF2.2)
- User-Space (represents the TSF SF2.1, SF2.1, SF3.1, SF4.1 and SF4.2)

Note: The references in brackets refer to the information given in the ST [6], chapter 6.1.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

Developer testing

The TOE was tested on a stand-alone computer which uses three virtual workstations. The TOE was running in a virtual machine which was configured according to chapter 1.2.2 of ST [6].

The tests of the TOE were carried out by executing the test environment. The virtual workstations resemble two standard workstations, one with the TOE installed.

The developer specified and implemented test cases for each defined subsystem. The test cases were divided into those of the TCP/IP Stack, the TCP/IP Filter, the Kernel-Space Kommunikation and User-Space. Thus all subsystems are covered by several test cases and each SFR-enforcing module is covered by at least one test case.

For the tests of the TOE, the developer used the test environment with three virtual workstations. The test environment is supported by an executable bash script that starts up the virtual machines and initializes the complete test network. Then each test case is located in a separate bash script. The developer carried out interactive as well as non-interactive tests. Altogether there were 95 test cases covered by the test specification.

The results of the TOE tests prove the correct implementation. All test cases were executed successfully and ended up with the expected result.

Independent testing

For repeating the developer tests, the evaluators used the same configuration as used in the developer tests. The description of the required non-TOE hardware, software and firmware is described in section 1.2.2 of the ST [6], using a stand alone PC with Intel Xeon(R) CPU 4 x 3.0 GHz, 16 GB RAM, Ubuntu 18.04 LTS 64-bit with Docker and installed the virtualized test setup of the developer.

For the independent tests the evaluators used a TOE installed on real Hardware that was provided by the developer as described in the ST [6], on which the release version of the TOE was installed:

- Fujitsu PRIMERGY RX 1330-M4 (Model: RX1330 M4 LFF or RX1330 M4 SFF)
- Syslogic COMPACT81-S (Model: SDB/OEMS81120-SBC1)
- Fujitsu PRIMERGY RX2530-M5 (Model: RX2530 M5)
- Pyramid VarioFlex 2 HE (Model: VarioFlex 2 HE v2016),

These systems fulfil the minimum system requirements. All test statements are only based on these configurations.

The general setup is the same as the developers test setup, i.e. the TOE connects via Ethernet a source machine (SRC) and a destination machine (DST) and is further connected to a machine inside the management network (Management). The complete test environment runs on a single Linux Host PC system which has several physical network cards (network interfaces) available, i.e. it is possible to realize SRC, DST and Management on this machine.

The evaluators performed the installation procedure of the TOE, as described by the developer in the guidance document [8]. The evaluators repeated all developer tests. Additionally the evaluators performed independent tests. No deviation between the actual result and the expected result was found.

Penetration tests

Publicly known vulnerabilities have been collected. The applicability of each attack path has been considered for the configured TOE in the intended environment.

For the penetration tests the differential firewall analysis method was used. In this method one needs to be able to compare the traffic on the “outside” to the traffic on the “inside” in real-time and alert when this contradicts. Therefore, two monitoring points are placed logically in front and behind the packet filter. At the monitoring points a sniffer is placed at which the network traffic is analysed.

The sensor that is placed on the “inside” alerts if traffic is detected and violating the firewall rules. In the operational environment of the TOE it is also possible that malicious or unintended traffic is coming from the inside of the network passing the TOE. It was tested that the packet filter responds to both network interfaces in the same way. The tests shall show if the TOE is resistant to attacks.

After the setup of the test environment different attack scenarios were defined. The attack scenarios were mapped to test cases and executed in the test environment.

For the penetration tests the evaluators used a TOE installed on real Hardware as described above. The test network was realized using virtualized source and destination machines. The host machine also provides the management network functionality.

Linux Host System (Hosting SRC, DST and Management)

- Hardware: Intel Xeon(R) CPU 4 x 3.0 GHz, 16 GB RAM
- Software: Ubuntu 18.04 LTS 64-bit OS and additionally software packages (VirtualBox, Wireshark, ntpd, rsyslog)

SRC (virtualized guest on the Linux Host)

- Hardware: This machine is virtualized and uses the host’s HW
- Software (OS): Debian GNU/Linux Version 10 (buster) 64-bit and additional pentest tools installed

DST (virtualized guest on the Linux Host)

- Hardware: This machine is virtualized and uses the host’s HW
- Software (OS): Debian GNU/Linux Version 10 (buster) 64-bit and additional pentest tools installed

The following list gives a short overview about the attack scenarios which have been tested or examined by design and code analysis:

- Port scan with or without different source ports to detect open ports.
- Bypassing the packet filter with fuzzy generated TCP, UDP or ICMP packets or during startup/shutdown.
- Bypassing the packet filter with a flood attack with “syn” or fragmented packets.
- Bypassing the packet filter with packets with a spoofed source address.
- Bypassing the packet filter due to IP-Range conflicts.
- Bypassing the packet filter and logging due to heavy load.
- Bypassing the access rule checks.

The TOE purposely reduces system logs in cases of heavy network load.

As a result, it can be assumed that the SFRs are implemented correctly and that they cannot be bypassed, deactivated or manipulated. The tested SFRs are listed in the following:

- FDP_IFF.1 Simple security attributes
- FAU_GEN.1 Audit data generation
- FMT_SMR.1 Security roles

The remaining SFRs were analysed but not tested through penetration due to non-exploitability of the related attack scenarios in the TOE's operational environment.

The overall test result is that no deviations were found between the expected and the actual test results. Please note, that the TOE is able to reduce syslog messages in cases of heavy network load and extensive set logging rules. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in Security Target [6] assumed that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE is defined by the notation "secunet wall Version 6.1.0" provided by secunet Security Networks AG with the components and hash values for the TOE as given in chapter 2. The TOE has to be configured following the TOE guidance [8]. There exists only one configuration of the TOE. The TOE was tested and thus shall be operated on one of the following hardware:

- Fujitsu PRIMERGY RX 1330-M4 (RX1330 M4)
- Syslogic COMPACT81-S (Model: SDB/OEMS81120-SBC2)
- Fujitsu-PRIMERGY RX 2530-M5 (Model: RX 2530-M5)
- Pyramid VarioFlex 2 HE (Model: VarioFlex 2 HE v2016)

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

The user must not load any new modules into the kernel. In case a new module is loaded the TOE is no longer in the certified configuration.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.2, AVA_VAN.5 und ASE_TSS.2 augmented for this TOE evaluation.

The evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1116-2020. The focus of this re-evaluation was on several functional, security, and design updates and enhancements.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.2, AVA_VAN.5 und ASE_TSS.2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Cryptographic primitive	Hashing for Password and signature Verification using SHA-256, SHA-512	[FIPS_180-4]	-	-	FCS_COP.1/SHA SHA-256 is used for container authentication. SHA-512 is used for password hashing.
2	Authenticity	RSA Signature verification with SHA-256 of the container signature	[IETF RFC 8017] [FIPS_180-4]	4096 bit	Yes	FCS_COP.1.1/RSA-verify

Table 3: TOE cryptographic functionality

References to the Table above:

- [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.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

The user must not load any new modules into the kernel. In case a new module is loaded the TOE is no longer certified.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation

cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DST	Destination
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HW	Hardware
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDAP	Lightweight Directory Access Protocol
OS	Operating System
OSI	Open Systems Interconnection
PGP	Pretty Good Privacy
PP	Protection Profile
RSA	Rivest Shamir Adleman
SAR	Security Assurance Requirement
SBC	Session Border Controller
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithms
SRC	Source
ST	Security Target
SW	Software
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Data Protocol

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1116-V2-2022, secunet wall 6.1.0, Version 1.1, Date 25.02.2022, secunet Security Networks AG

[7] Evaluation Report secunet wall 6.1.0, BSI-DSZ-CC-1116-V2, Version 1.6, Date: 05.04.2022, SRC Security Research & Consulting GmbH (confidential document)

[8] secunet wall 6.1.0, Administrationshandbuch,, Handbuch-Version 1.1, 25.02.2022, secunet Security Networks AG

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)

[9] Release Notes secunet wall 6.1.0.2, Datum: 25.02.2022, secunet Security Networks AG

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report