Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1016-2020

for

Sophos Firewall OS Version 17.0

from

Sophos Ltd.

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-1016-2020 (*)

Firewall

Sophos Firewall OS Version 17.0

from	Sophos Ltd.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 extended EAL 4 augmented by ALC_FLR.3

SOGIS
Recognition Agreement

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 for 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 4

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, 18 February 2020

For the Federal Office for Information Security

Bernd Kowalski
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 BSIG1 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]
- BSI Schedule of 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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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 under SOGIS-MRA for all assurance components selected.

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: http://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 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] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 Sophos Firewall OS Version 17.0 has undergone the certification procedure at BSI.

The evaluation of the product Sophos Firewall OS Version 17.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 5 February 2020. 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: Sophos Ltd.

The product was developed by: Sophos Ltd.

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 18 February 2020 is valid until 17 February 2025. Validity can be re-newed by re-certification.

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,

[5] Information Technology Security Evaluation Facility

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 Sophos Firewall OS Version 17.0 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] Sophos Ltd.
The Pentagon, Abington Science Park
OX14 3YP Abington
UK

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 Sophos Firewall OS Version 17.0 which is a part of the Sophos Firewall OS v17.0. The TOE enforces packet filtering rules defined by an administrator. Administrators can log in at a web interface and set these packet filtering rules. The administrators are considered end-users of the TOE. The guidance documentation [8] and the Reference Guide [9] are intended to be used by the TOE administrators. The TOE relies on information available at OSI layer 3 and layer 4 for policy enforcement. The product Sophos Firewall OS v17.0 supports IPv4 and IPv6. In scope of the evaluation is the IPv4 security functionality. The TOE provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse. These logs can be viewed through the Web Admin Console.

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.3.

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

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

TOE Security Functionality	Addressed issue
Security Audit functionality	The Security Audit function provides the TOE with the functionality for generation, storage, and viewing of audit records. As administrators manage and configure the TOE, their activities are tracked by recording audit records into the logs. All security-relevant configuration changes are recorded to ensure accountability of the administrator’s actions. All logs contain the time, device, type of event, log ID, and priority. Firewall log files additionally contain component, action, username, firewall rule, incoming interface, outgoing interface, source IP, and destination IP.
User Data Protection	The security policy of an organization in the context of computer networking is a set of rules to protect the computer networks of an organization and the information that goes through it. By default, the TOE denies all packets that are not specifically allowed. The TOE enables the administrator of the TOE to add a policy. Through the use of policies, the administrator configures a set of firewall rules that tell the TOE to allow or deny traffic based upon factors such as source and destination of the packet, port number, as well as the transport protocol type. Transport

TOE Security Functionality	Addressed issue
	protocol that can be filtered are TCP and UDP.
Identification and Authentication	The Identification and Authentication functionality establishes and verifies a claimed administrator identity. The TOE requires successful identification and authentication of all users (administrator) before allowing access to any management functionality of the Web Admin Console. The TOE provides the identification and authentication mechanism by means of a PostgreSQL database for storing the credentials. This ensures that the user has the appropriate privileges associated with the assigned profile. Only authenticated users are allowed access to the TOE and TOE security functions. Users must be identified and authenticated prior to performing any TSF-mediated actions on the TOE. For each user, the TOE stores the following security attributes locally: username, password, and profile. When a TOE user enters a username and password at the Web Admin Console, the information is passed to the TOE, where it is verified against the username and password stored in the TOE. If the provided username and password match, the TOE administrator is assigned the roles associated with that username.
Security Management	The Security Management function specifies the management of several aspects of the TSF, including security function behaviour and security attributes. The TOE allows administrators to create profiles for various administrator users. Profiles are a function of an organization's security needs and can be set up for special-purpose administrators in areas such as firewall administration, network administration, and logs administration. A profile separates the TOE's features into access control categories for which an administrator can enable none, read only, or read-write access.
TOE Access	The TOE Access function specifies requirements for controlling the establishment of an administrator's session, which is configured by Administrator roles with sufficient permission level. The TSF terminates an administrator's interactive session after a configurable time interval of administrator inactivity at the Web Admin Console, the default time interval is 10 minutes. Additionally, the Administrator can terminate the interactive session by himself. If an administrator's session is timed out, the administrator must log back in to the TOE to perform any further functions.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.

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 and 4.

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:

Sophos Firewall OS Version 17.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Sophos SFOS 17.0.10 MR-10 (for the hardware appliance)	Software (binary) HW-SFOS_17.0.10_MR-10-240.iso SHA-256 hash sum: 65875f5d8c1dcda770d613bc9b100273a00b0de02e96e4c062c10ea6ee9fd589	Secure Download
2	SW	Sophos SFOS 17.0.10 MR-10 (for the virtual appliance)	Software (VMware image folder) VI-SFOS_17.0.10_MR-10.VMW-240.zip SHA-256 hash sum: 7aa46e24063a13d5abe832a860cc61117f63521dc149cbbe696a351ee6db2224	Secure Download
3	DOC	Guidance Documentation Supplement Sophos Firewall OS Version 17.0	Guidance Documentation [8] AGD_sophos_sfos_v1.00.pdf SHA-256 hash sum: 35fa0b4fec074117d2b3bfcdac2cddf65c58a1fa0f286948c4dc93d60624d7e3	Secure Download

No	Type	Identifier	Release	Form of Delivery
4		Sophos XG Firewall Web Interface Reference and Admin Guide v17	Guidance Documentation [9] Sophos XG Firewall Web Interface Reference Guide.pdf SHA-256 hash sum: 0863d5e153da76961f45191eeffecaa15d71a6928bb819fd6652665e70d7103c	Secure Download

Table 2: Deliverables of the TOE

The TOE can be downloaded from the Sophos website:

https://www.sophos.com/en-us/mysophos/my-account/network-protection/common-criteria-installers.aspx

The TOE can be identified by the end user (i.e. the administrator of the TOE). This identification can be done by any tool that can calculate the SHA-256 hash sum of a file e.g. GnuPG. This calculation must be done on the downloaded file (see above) and then the calculated hash must be compared to the SHA-256 hash sums listed in the ST and this report. If the hash values match the user can be sure that he has received the certified TOE.

To verify that the correct version is installed the administrator use the Web Admin Console as described in [8], chapter 2.2.2.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the issues Security Audit functionality, User Data Protection, Identification and Authentication, Security Management and TOE Access.

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. Details can be found in the Security Target [6], chapter 4.

5. Architectural Information

The TOE is firmware with firewall and gateway functionality that runs on Sophos series hardware and virtual appliances.

The TOE is separated into various subsystems and modules that provide the TOE Security Functions. The TOE boundary consists of the Sophos Firewall OS Version 17.0 and does not include the hardware appliance or virtual appliance on which the firmware resides, nor the items excluded in Sophos Firewall OS Version 17.0 Security Target. The boundary includes the subsystems Control & Configuration Subsystem, Network Traffic Subsystem, Audit Subsystem, Core Subsystem and the external interfaces Web Admin Console and Network Traffic In Interface.

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

7.1. Developer Testing

The developer tested all TOE Security Functions. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby, a representative sample including all boundary values of the parameter set were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

TOE Test Configuration

The TOE evaluation contains two configurations: The hardware appliance and the virtual appliance. The used test system for the hardware appliance consists of Sophos XG 115, Client A / Syslog Server, and Client B. After the installation according chapter 2.2.2.1 of [8] the TOE was set up according to chapter 2.2.3 of [8] to achieve the evaluated configuration.

The used test system for the virtual appliance consists of Sophos SFOS 17.0 MR-10 VMWare image, Client A / Syslog Server, and Client B. The TOE has been set up as a virtual machine in VirtualBox 6.0.4. The two Clients, Client A and Client B are also set up as virtual machines running Ubuntu 18.04. After the installation according chapter 2.2.2.2 of [8] the TOE was set up according to chapter 2.2.3 of [8] to obtain the evaluated configuration. This configuration is consistent with the one used by the developer.

Testing Approach

The developer tests were divided in two groups, where the first group covers all security functional requirements (SFRs) defined in the ST [6] and the second group covers all second order TSFIs from the user interface. All developer tests were executed manually.

Conclusion

All test cases were executed successfully and ended up with the expected result.

7.2. Evaluator Independent Testing

TOE Test Configuration

The independent testing was performed using the same test setup as described above. Both configurations, “Hardware Appliance Configuration” and “Virtual Appliance Configuration” as described above were tested.

Testing Approach

For the repetition of the developer tests the evaluators used the test setups for the “Hardware Appliance Configuration” and for the “Virtual Appliance Configuration” as described above.

The evaluators implemented additional test cases for all interfaces. Test cases devised by the evaluators include Conflicting Firewall Rules tests to check whether conflicting firewall rules are treated correctly, UDP Bypass tests to check, whether UDP Bypass rules are applied, and Trusted MAC tests to check whether the MAC Filter feature of the Spoof Prevention Mechanisms works correctly.

Conclusion

All tests were executed successfully. No deviation between the actual result and the expected result was found.

7.3. Evaluator Penetration Testing

TOE Test Configuration

The penetration testing was performed using the same test setup as described above. Both configurations, “Hardware Appliance Configuration” and “Virtual Appliance Configuration” as described above were used.

Testing Approach

The evaluator created a list of potential vulnerabilities based on the results gained while performing the AVA work units. On the base of this analysis, several possible attack scenarios have been tested, such as

- Find open ports with Port Scan of Network Traffic In Interface. The *Nessus Professional Vulnerability Scanner* was used to perform an advanced scan with TCP port range from 0 to 65535 and UDP port range from 0 to 1000.
- The packet filter was tested manually by sending TCP or UDP packets from Client A using *netcat* and *mausezahn*. Client B listens for incoming traffic using *netcat* and *Wireshark*. While doing this, different packet filter settings like adding and removing rules or changing the order of rules in the Web Admin Interface were tested.
- Test cases that target bypassing web authentication, performing SQL injection, and performing cross-site-scripting.
- The Web Admin console was scanned using *Burpsuite Professional*. During the manual and semi-automated tests, the web admin console was tested randomly for critical web application flaws and vulnerabilities like SQL injection, JSP template injection, Command injection, Cross-site-scripting , Upload vulnerabilities, Session handling flaws, XML External Entities, and insecure user permissions. Using a HTTPS-Proxy like *Burpsuite Professional* or *Zed Attack* Proxy, the requests made by Client A while using the Web Admin Console were observed.
- The evaluators and the developer performed a CVE analysis on the Linux kernel and also on used open source components. Also the CVEs of the other open source components besides the kernel were analysed by the developer. The result was that either potential vulnerabilities were fixed by the developer or the CVEs were not relevant for the TOE in its intended environment and configuration.
- Tests using the *hping3* tool to send a big amount of data to the TOE were performed. The evaluators verified that in an overload situation the number of blocked packets still matches the number of total packets sent and that the TOE does not produce unpredictable results.

Conclusion

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential enhanced basic was actually successful in the TOE's operational environment as defined in the ST [6]. The test results fulfil the requirements of AVA_VAN.3.

8. Evaluated Configuration

The TOE can be applied in two configurations, i.e. to run on hardware (HW-SFOS_17.0.10_MR-10-240.iso in table 2 above) and run as a VMware image (VI-SFOS_17.0.10_MR-10.VMW-240.zip in table 2 above). For the certified version, the hardware appliance XG 115 is in scope of the certified configuration. For the VMware package the requirements as detailed in the ST [6] chapter 1.2.2 apply. Chapter 1 of the ST [6] gives comprehensive information on the TOE boundaries, configuration, requirements and functions covered and excluded from the certification. Table 2 above and chapter 2 of this report give information about the TOE items and their identification.

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.

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.3 augmented for this TOE evaluation.

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 extended
  EAL 4 augmented by ALC_FLR.3

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 TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

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.

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.

In addition, the following aspects need to be fulfilled when using the TOE:

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

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. Definitions

12.1. 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
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HW	Hardware
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JSP	Java Server Pages
MAC	Media Access Control
OS	Operating System
OSI	Open Systems Interconnection

PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SQL	Structured Query Language
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UDP	User Datagram Protocol
XML	Extensible Markup Language

12.2. 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.

13. 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
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, http://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-1016-2020, Sophos Firewall OS Version 17.0, Version 1.00, Sophos Ltd., 2020-02-04

[7] Evaluation Technical Report, Version 1.2, 05.02.2020, Sophos Firewall OS Version 17.0, SRC Security Research & Consulting GmbH (confidential document)

[8] Guidance Documentation Supplement Sophos Firewall OS Version 17.0, Version 1.00, Sophos Ltd. 2020-02-04, file name: AGD_sophos_sfos_v1.00.pdf

[9] Sophos XG Firewall Web Interface Reference and Admin Guide v17, March 2018, Sophos Ltd., file name: Sophos XG Firewall Web Interface Reference Guide.pdf

[7] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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 detailled 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 http://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