Agenzia per la Cybersicurezza Nazionale

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Il prodotto identificato in questo certificato è risultato conforme ai requisiti ISO/IEC 15408 Common Criteria (CC) v.3.1 rel. 5

Certificato n. *(Certificate No.)*	03/2024
Rapporto di Certificazione *(Certification Report)*	OCSI/CERT/CCL/13/2021/RC, v1.0
Decorrenza *(Date of 1st Issue)*	26 febbraio 2024
Nome e Versione del Prodotto *(Product Name and Version)*	Sophos Firewall OS v19.0.2-MR-2-Build472
Sviluppatore *(Developer)*	Sophos Ltd
Tipo di Prodotto *(Type of Product)*	Rete e Dispositivi e Sistemi relativi alla rete
Livello di Garanzia *(Assurance Level)*	EAL4+ (ALC_FLR.3) conforme a CC Parte 3
Conformità a PP *(PP Conformance)*	Nessuna
Funzionalità di sicurezza *(Conformance of Functionality)*	TDS specifico per il prodotto conforme a CC Parte 2

Riconoscimento CCRA per componenti fino a EAL2 e solo ALC_FLR
(CCRA recognition for components up to EAL2 and ALC_FLR only)

Riconoscimento SOGIS MRA per componenti fino a EAL4
(SOGIS MRA recognition for components up to EAL4)

Roma, 26 febbraio 2024

Il Capo Servizio
Certificazione e Vigilanza
(A. Billet)

[ORIGINAL SIGNED]

Il prodotto IT (*Information Technology*) identificato nel presente certificato è stato valutato presso un LVS (Laboratorio per la Valutazione della Sicurezza) accreditato e abilitato/approvato utilizzando la Metodologia Comune per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5 per la conformità ai Criteri Comuni per la Valutazione di Sicurezza della Tecnologia dell'Informazione versione 3.1 revisione 5. Questo certificato si applica solo alla versione e al rilascio specifici del prodotto nella sua configurazione valutata e unitamente al Rapporto di certificazione completo. La valutazione è stata condotta in conformità alle disposizioni dello Schema nazionale per la valutazione e la certificazione della sicurezza nel settore della tecnologia dell'informazione (DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004) e le conclusioni dell'LVS nel Rapporto di Fine Valutazione sono coerenti con le evidenze addotte. Il presente Certificato non costituisce un sostegno o promozione del prodotto IT da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosca o dia effetto a questo certificato, e nessuna garanzia del prodotto IT, da parte della Agenzia per la Cybersicurezza Nazionale o di qualsiasi altra organizzazione che riconosce o dà effetto a questo certificato, è espressa o implicita.

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using Common Methodology for Information Technology Security Evaluation version 3.1 release 5 for conformance to *Common Criteria for Information Technology Security Evaluation version 3.1 release 5. 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. The evaluation has been conducted in accordance with the provisions of the National scheme for the evaluation and certification of the security in the sector of information technology (Prime Ministerial Decree of 30 October 2003 - Official Journal no. 93 of 27 April 2004) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product, by Agenzia per la Cybersicurezza Nazionale or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.*

Agenzia per la Cybersicurezza Nazionale

Servizio Certificazione e Vigilanza

Organismo di Certificazione della Sicurezza Informatica

Certification Report

Sophos Firewall OS v19.0.2-MR-2-Build472

OCSI/CERT/CCL/13/2021/RC

Version 1.0

26 February 2024

Courtesy translation

Disclaimer: This English language translation is provided for informational purposes only. It is not intended to substitute the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	26/02/2024

2 Table of contents

3 Acronyms

3.1 National scheme

DPCM	Decreto del Presidente del Consiglio dei Ministri
LGP	Linea Guida Provvisoria
LVS	Laboratorio per la Valutazione della Sicurezza
NIS	Nota Informativa dello Schema
OCSI	Organismo di Certificazione della Sicurezza Informatica

3.2 CC and CEM

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SOGIS-MRA	Senior Officials Group Information Systems Security – Mutual Recognition Agreement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

3.3 Other acronyms

CLI	Command Line Interface
DMZ	Demilitarized Zone
GPC	General Purpose Computer

HTTPS	Hyper Text Transfer Protocol Secure
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
NTP	Network Time Protocol
OS	Operating System
OSI	Open Systems Interconnection
PC	Personal Computer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

4 References

4.1 Normative references and national Scheme documents

[CC1] CCMB-2017-04-001, "Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model", Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, "Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components", Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, "Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components", Version 3.1, Revision 5, April 2017

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

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

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

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

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

[NIS1] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 1/23 – Modifiche alla LGP1, versione 1.1, 21 agosto 2023

[NIS2] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 2/23 – Modifiche alla LGP2, versione 1.1, 21 agosto 2023

[NIS3] Organismo di certificazione della sicurezza informatica, Nota Informativa dello Schema N. 3/23 – Modifiche alla LGP3, versione 1.1, 21 agosto 2023

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

4.2 Technical documents

[CC_GUIDE] Sophos Firewall OS v19.0.2 Guidance Documentation Supplement, version 0.5 November 16th 2023

[ETR1] Evaluation Technical Report, Sophos Firewall OS v19.0.2-MR-2-Build472, SOPHOS-029-ETR_v2, CCLab Software Laboratory, 5 December 2023

[ETR2] Evaluation Technical Report, Sophos Firewall OS v19.0.2-MR-2-Build472, SOPHOS-029-ETR_v4, CCLab Software Laboratory, 22 January 2024

[ST] Sophos Ltd. Sophos Firewall OS v19.0.2 Security Target, version 0.9, November 16th 2023

5 Recognition of the certificate

5.1 European recognition of CC certificates (SOGIS-MRA)

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

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

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

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

5.2 International recognition of CC certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] was ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

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

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

This certificate is recognised under CCRA up to EAL2 and ALC_FLR only.

6 Statement of certification

The Target of Evaluation (TOE) is the product named "**Sophos Firewall OS v19.0.2-MR-2-Build472**", developed by Sophos Ltd.

The TOE is a software-only network firewall that runs on the Sophos XGS series hardware and virtual appliances. The firewall functionality, by means of a set of rules, protects the network from unauthorized access and typically prevents malicious access to LANs and Demilitarized Zone (DMZ) networks.

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

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

The TOE resulted compliant with the requirements of Part 3 of the CC version 3.1 Revision 5 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [ST] and in the configuration shown in "Annex B – Evaluated configuration" of this Certification Report.

The TOE certified configuration consists of the TOE operating on the hardware models and virtual appliances listed in Appendix A, Tables 21 and 22 of the Security Target [ST]. The different hardware models in the listed series differ in terms of performance level, additional connectivity and port availability.

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

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product named "Sophos Firewall OS v19.0.2-MR-2-Build472" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

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

7.2 Executive summary

TOE name	Sophos Firewall OS v19.0.2-MR-2-Build472
Security Target	Sophos Firewall OS v19.0.2-MR-2-Build472 - Security Target, Sophos Ltd, version 0.9, November 16th 2023
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	Sophos Ltd
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory - Budapest site
CC version	3.1 Rev. 5
PP conformance claim	No conformance claimed
Evaluation starting date	15 November 2021
Evaluation ending date	5 December 2023

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

7.3 Evaluated product

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

The Target of Evaluation (TOE) is the product named "Sophos Firewall OS v19.0.2-MR-2-Build472", developed by Sophos Ltd.

The TOE is a software-only network firewall that runs on the Sophos XGS series hardware and virtual appliances.

To control Internet access entirely through the TOE, the entire Internet bound traffic from the Local Area Network (LAN) must first pass through the TOE. The firewall functionality, by means of a set of rules, protects the network from unauthorized access and typically prevents malicious access to

LANs and Demilitarized Zone (DMZ) networks. Firewall rules may be also configured to limit access to harmful sites for LAN users.

Firewall rules provide centralized management of security policies. From a single firewall rule, the user can define and manage an entire set of TOE security policies. Firewall rules control traffic passing through the TOE. Depending on the instruction in the rule, the TOE decides on how to process the access request. When the TOE receives the request, it checks for the source address, destination address, TCP or UDP protocol, and port number and tries to match it with the firewall rule. It also keeps track of the state of connection and denies any traffic that is not part of the connection.

The packet filter that is part of the Sophos Firewall OS relies on information available at OSI layer 3 and layer 4 for policy enforcement. The Sophos Firewall OS supports IPv4 and IPv6. In scope of the TOE there is only IPv4 security functionality.

For a detailed description of the TOE, refer to sections 1.3 and 1.4 of the Security Target [ST].

7.3.1 TOE architecture

The TOE is a software-only network firewall that runs on the Sophos XGS series hardware and virtual appliances (see models listed in Appendix A of the security Target [ST]) compliant to the minimum requirements as listed in Table 2 of the Security Target [ST].

The TOE is installed on a network whenever firewall services are required as depicted in Figure 1 and Figure 2.

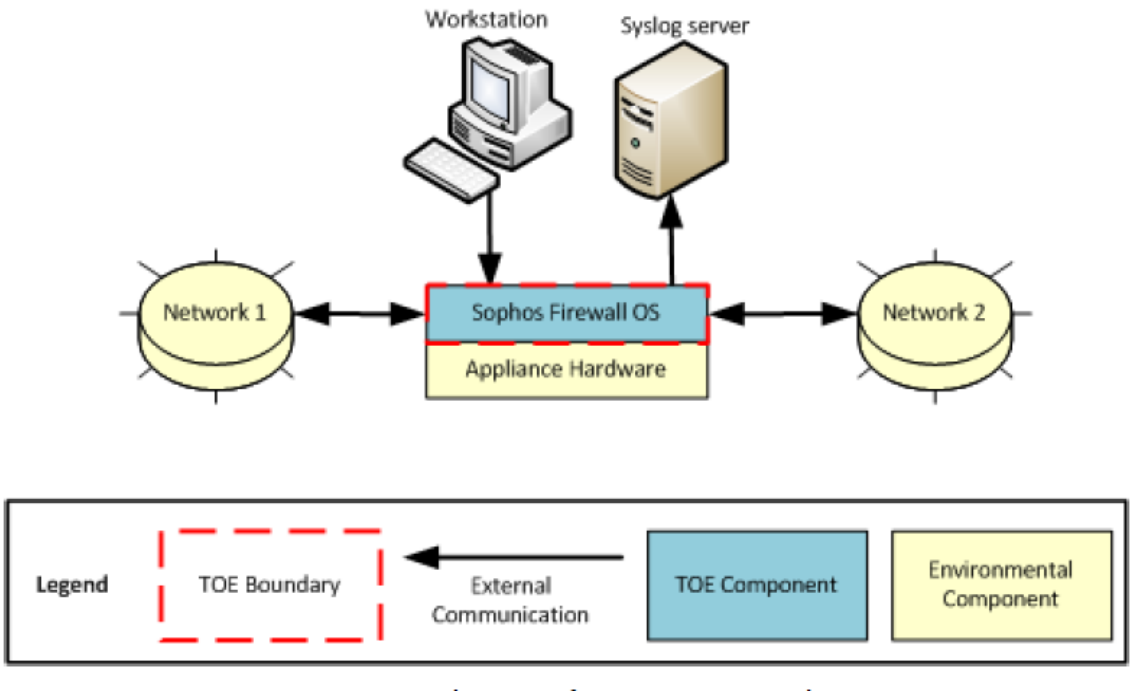

Figure 1 - Hardware Configuration TOE Boundary

The physical components of the operational environment in the evaluated configuration for the TOE are:

- When the TOE is installed on Sophos XGS series hardware:
  - Workstation.
  - Syslog server.
  - Appliance hardware (Sophos XGS series hardware) for the TOE.
  - The network components for the separate networks (Network 1 e Network 2).
- When the TOE is installed on the virtual appliance:
  - Workstation.
  - Syslog server.
  - Hypervisor.
  - General Purpose Computer for hypervisor.
  - The network components for the separate networks (Network 1 e Network 2).

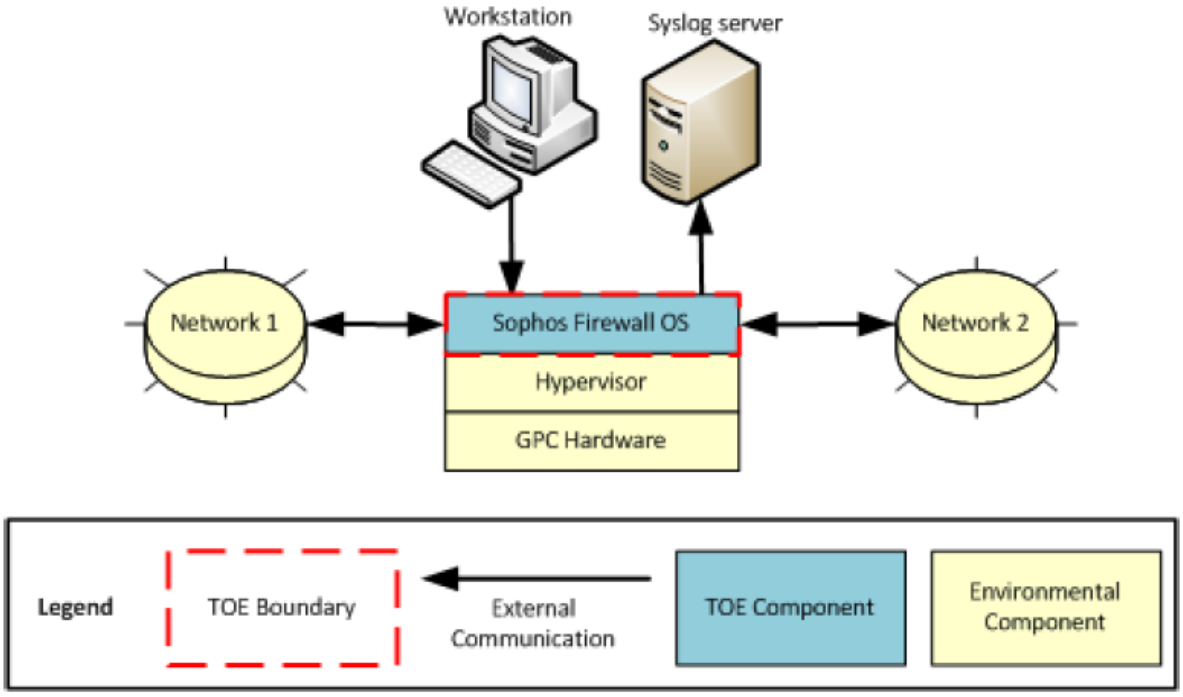

Figure 2 - Virtual Configuration TOE Boundary

The TOE includes the following subsystems:

- Control & Configuration Subsystem.
- Network Traffic Subsystem.
- Audit Subsystem.
- Core Subsystem.

The Control & Configuration Subsystem provides the management component of the TOE and a web-based interface.

The Network Traffic Subsystem is responsible for receiving network traffic, performing the appropriate processing and sending the traffic to its destination.

The Audit Subsystem is responsible for receiving, formatting, and storing auditable events generated by other subsystems within the TOE.

The Core Subsystem provides the general-purpose Operating System (OS) functionality that is required for the TOE operation.

7.3.2 TOE security features

Assumptions, threats and security objectives are defined in section 3 and 4 of the Security Target [ST].

The security functional requirements implemented by the TOE are grouped under the following Security Function Classes:

- Security Audit.
- User Data Protection.

- Identification and Authentication.
- Security Management.
- TOE Access.

For a detailed description of the TOE Security Functions, refer to sections 1.4.2 and 7 of the Security Target [ST]. The most significant aspects are summarized in the following sections.

7.3.2.1 Security Audit

The TOE generates audit records for the startup and shutdown of the audit functions along with audit records for firewall functionality and administration activity. An Administrator or Audit Admin can view, search, and filter the audit records based on different factors that vary between Admin and Firewall log files. The TOE protects audit records in the audit trail from unauthorized deletion and modification by limited which profiles have access to the audit records and by uploading logs to the external syslog server for redundancy. All historical audit records are maintained and stored in the external syslog server.

7.3.2.2 User Data Protection

The TOE controls data sent through the TOE from one external entity to another via the Traffic Information Flow Control SFP. The Traffic Information Flow SFP relies on source and destination IP addresses, TCP or UDP protocol, port numbers, and rules defined in the Traffic Information Flow Control List to determine how to treat the network traffic. The rules determine whether traffic should be accepted through the TOE to its destination, or if the traffic should be dropped/rejected.

7.3.2.3 Identification and Authentication

TOE users are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. The TOE limits unsuccessful login attempts from an IP address to prevents unauthorized entities from gaining access to the TOE. This feature is configurable and allows a settable number of unsuccessful logins and settable lockout timer.

7.3.2.4 Security Management

The TOE offers a Web Admin Console that TOE users can use to configure and manage specific TOE settings, manage the firewall runs and the Traffic Information Flow Control SFP, configure authentication protection, manage users, and use the Log Viewer. The TOE supports different profiles: Administrator, Audit Admin, and Security Admin. The Administrator and Security Admin profiles have the ability to modify and delete the restrictive default security attributes for the Traffic Information Flow Control SFP. The Audit Admin profile has the ability to monitor the logs and modify reports of the TOE.

7.3.2.5 TOE Access

A TOE user can terminate their own interactive session. An Administrator or Security Admin can configure the TOE to display a warning message regarding unauthorized use of the TOE before an authentication session occurs.

7.4 Documentation

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

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

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

7.5 Protection Profile conformance claims

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

7.6 Functional and assurance requirements

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

All the SFRs have been selected or derived by extension from CC Part 2 [CC2].

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

7.7 Evaluation conduct

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

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

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

The evaluation was completed on 5 December 2023 with the issuance by the LVS of the Evaluation Technical Report [ETR1], which was approved by the Certification Body on 4 January 2024. A final version of the ETR was delivered by the LVS on 22 January 2024 [ETR2] including minor changes. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [ST], with reference to the operational environment specified therein. The evaluation has been performed on the TOE configured as described in "Annex B – Evaluated configuration".

Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

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

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [ETR1] issued by the LVS CCLab Software Laboratory (Budapest site) and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE named "Sophos Firewall OS v19.0.2-MR-2-Build472" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4 augmented with ALC_FLR.3, with respect to the security features described in the Security Target [ST] and the evaluated configuration, shown in "Annex B – Evaluated configuration".

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4 augmented with ALC_FLR.3 (augmentation in italics in Table 1).

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

Assurance classes and components		Verdict
Well-defined development tools	ALC_TAT.1	Pass
Systematic flaw remediation	*ALC_FLR.3*	*Pass*
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 Final verdicts for assurance requirements

8.2 Recommendations

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

Potential customers of the product "Sophos Firewall OS v19.0.2-MR-2-Build472" are suggested to properly understand the specific purpose of the certification by reading this Certification Report together with the Security Target [ST].

The TOE must be used according to the "Security Objectives for the Operational Environment" specified in section 4.2 of the Security Target [ST]. It is assumed that, in the operational environment of the TOE, all Assumptions described in section 3.3 of the Security Target [ST] shall be satisfied.

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

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

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

9.1 TOE delivery

The Sophos XGS series hardware are shipped from the warehouses to the customer address as provided in the order using an international common carrier with a tracking system.

Each Sophos XGS series hardware is uniquely labelled (see Figure 3) and provides information on the model and a numeric version number.

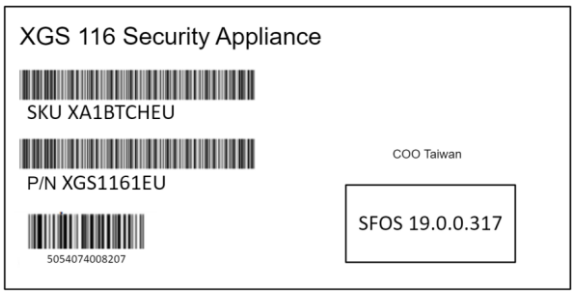

Figure 3 - Sample Packaging Label

TOE for Sophos XGS series hardware and virtual appliances are delivered to customers using the Sophos Support Portal.

In addition, the TOE documentation can be also downloaded from the Sophos Support Portal. The user can verify the Guidance documentation version by checking the version number printed in the document.

The Sophos Support Portal contains a webpage[1] where the specific version of the TOE (v19.0.2-MR-2-Build472) Common Criteria certified can be downloaded. In particular, the webpage contains the Common Criteria section with the ISO images for Sophos XGS series hardware and files for virtual appliances.

In order to check the integrity of the TOE, which is downloaded, it is possible to compare the hash calculated on the downloaded TOE with the following strings:

- Sophos XGS series hardware
  HW-19.0.2_MR-2-472.iso
  SHA256: A67BD740374BA348CD4183AABCB2388FE50F58E5DE6A0E5FF2C9FF8B75188003
- VMware virtual appliance
  VI-19.0.2_MR-2.VMW-472.zip
  SHA256: 11AAC8BA9B95C5A62D5E2E46FC66F58E84F0EC2C5C84288DD4EC9D2A4C45F030
- Hyper-V virtual appliance
  VI-19.0.2_MR-2.HYV-472.zip
  SHA256: 95D115FDDE194FE279CBCE0890B66625BDB1A04053FA44BCC3D259E5D5E02EB6
- KVM virtual appliance
  VI-19.0.2_MR-2.KVM-472.zip
  SHA256: 82C90A7C69EFCF6F7B63C015246554230F3117A606B7B02BFAC78A99EEAE13D2

[1] https://www.sophos.com/en-us/support/downloads/firewall-installers

- XenServer virtual appliance
  VI-19.0.2_MR-2.XEN-472.zip
  SHA256: 093C0C3D3C20529A8782FA417F899EED40FB4EAF0C42E7598D7D612E7D329455

9.2 Installation, configuration and secure usage of the TOE

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

In particular, the document [CC_GUIDE] contains detailed information for the secure initialization of the TOE, the preparation of its operational environment and the secure usage of the TOE in accordance with the security objectives specified in the Security Target [ST].

The user can verify TOE version after installation by checking the installed version as described in [CC_GUIDE].

10 Annex B – Evaluated configuration

The Evaluators followed the preparation steps defined in the [CC_GUIDE] for the TOE being in the evaluated configuration.

The TOE certified configuration consists of the TOE operating on the hardware models and virtual appliances listed in Appendix A, Tables 21 and 22 of the Security Target [ST]. The different hardware models in the listed series differ in terms of performance level, additional connectivity and port availability. Two instances of the TOE were tested by the evaluation facility (LVS). One was run on a Sophos XGS hardware (XGS 3100) and one on a virtual appliance using virtualization software (VMware ESXi) installed on a General Purpose Computer. Moreover, no TSF related deviations were identified by LVS during the evaluation process between the two instances.

The items described in section 10.1 "TOE operational environment" must be available before performing the installation.

10.1 TOE operational environment

The following components are part of the TOE environment:

- Sophos XGS series hardware (only for hardware installation).
- Local workstation used by administrators for accessing Web Admin Console of the TOE.
- Syslog Server to store and maintain audit records.
- General Purpose Computer to install the Hypervisor (only for virtual installation).
- Hypervisor software (only for virtual installation).
- General Purpose Computers that send and/or receive information through the TOE.

11 Annex C – Test activity

This annex describes the task of both the Evaluators and the Developer in testing activities.

11.1 Test configuration

Two instances of the TOE were tested by the evaluation facility (LVS). One was run on a Sophos XGS hardware (XGS 3100) and one on a virtual appliance using virtualization software (VMware ESXi) installed on a General Purpose Computer.

Testing activities were carried out in the LVS site and the Evaluators verified the configuration of the test environment, including the two instances of TOE, and found them consistent with the Common Criteria Preparative Procedures [CC_GUIDE] and the Security Target [ST].

11.2 Functional tests performed by the Developer

11.2.1 Testing approach

The Developer covered all the TSFIs with at least one test case. For each test case, the Developer's test documentation describes its purpose, the relevant TSFI(s) and SFR(s), test prerequisites, step-by-step test procedures, and expected test results.

The Developer created tests related to the following categories:

- Test case 01: Test Setup.
- Test case 02: Security Audit.
- Test case 03: User Data Protection.
- Test case 04: Identification and Authentication.
- Test case 05: Security Management.
- Test case 06: Default TOE Access Banners.
- Test case 07: Additional TSFI Test Cases.

11.2.2 Test coverage

The Evaluators verified the complete coverage between the test cases in the test documentation provided by Developer and the TSFIs described in the functional specification. The Evaluators verified that the test cases are sufficient to demonstrate the internal behaviour and properties of the TSF.

11.2.3 Test results

The actual test results of all Developer's tests were consistent with the expected ones.

11.3 Functional and independent tests performed by the Evaluators

11.3.1 Test approach

Upon reception of the Sophos XGS hardware, the Evaluators verified the item. They created a dedicated environment for testing the TOE in a virtual appliance.

The Evaluators installed the TOE downloaded from Sophos Support Portal (see section 9.1 TOE delivery) in the Sophos XGS hardware and in the virtual environment.

Before initiating the testing activity, the Evaluators verified that the TOE was configured correctly according to the guidance documentation provided together with the TOE ([CC_GUIDE]).

The Evaluators divided the execution of the Developer tests as follows:

- Test cases conducted on the Sophos XGS hardware:
  - Test case 01: Test Setup.
  - Test case 02: Security Audit.
  - Test case 03: User Data Protection.
- Test cases conducted on the virtual appliance:
  - Test case 04: Identification and Authentication.
  - Test case 05: Security Management.
  - Test case 06: Default TOE Access Banners.
  - Test case 07: Additional TSFI Test Cases.

Each Developer test case contains several sub-test cases and on the virtual appliance the Evaluators also conducted some sub-tests taken from Test Case 01, 02 and 03.

The Evaluators created the following independent test:

- SOPHOS001 - User creation functionality testing.
- SOPHOS002 - Permission testing.
- SOPHOS003 - Testing the firewall traffic rules.
- SOPHOS004 - Session timeout testing.
- SOPHOS005 - Unmodifiable security attributes testing.

11.3.2 Test results

All Developer's tests were run successfully and the Evaluators verified the correct behaviour of the TSFIs and TSFs and correspondence between expected results and achieved results for each test.

All test cases devised by the Evaluators were passed successfully and all the test results were consistent to the expected test results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities, the Evaluators worked with the TOE on the Sophos XGS hardware (XGS 3100) and virtual appliance already used for the functional test activities and verified that the TOE and the test environment were properly configured. Most recent vulnerability analysis was performed by Evaluators on November 10th, 2023.

The Evaluators designed the following attack scenarios:

- Privilege escalation.
- Command injection.

- Bypass of security attributes.
- Force unencrypted connection.
- Encryption vulnerability.
- Change of security attribute.
- Stored Cross Site Scripting.

The Evaluators sent an Observation Report to request to the Developer to correct some identified vulnerabilities. The TOE was updated by the Developer to fix the previously identified vulnerabilities; hence, the Evaluators repeated the penetration tests and they observed that the previous vulnerabilities were properly corrected by Developer.

The Evaluators has concluded that the TOE is resistant to Enhanced-Basic attack potential in its intended operating environment.