Sophos Ltd.

Sophos Firewall OS

v19.0.2

Guidance Documentation Supplement

Evaluation Assurance Level (EAL): EAL4+
Document Version: 0.5

Prepared for:

SOPHOS
Cybersecurity evolved.

Sophos Ltd.
The Pentagon
Abington Science Park
Abington OX14 3YP
United Kingdom

Phone: +1 866 866 2802
www.sophos.com

Prepared by:

Corsec

Corsec Security, Inc.
12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America
12600 Fair Lakes Circle, Suite 210

Phone: +1 703 267 6050
www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2022-06-01	Manil Trivedi	Initial draft.
0.2	2023-04-05	Ryan Butler	Corrected TOE version number from v19.0 to v19.0.0 in all cases Clarified that this document will be co-located with the TOE upon publication. Added missing XGS 7500/8500 Quick Start Guide to Table 2 Added Section 3.1.8 User Interfaces Added Section 3.1.9 TOE Modes of Operation Updated list of excluded features in Section 3.2 Removed section 3.3.1.3 General clarity fixes Updated Corsec mailing address on cover page and final page
0.3	2023-05-18	Cole Murphy	Updated Version to 19.0.2 Added section 3.1.10 Removed section 3.3.1.4 Added section 3.3.4 Troubleshooting and following subsections
0.4	2023-06-26	Cole Murphy	Document changed to Sophos Firewall 19.0 Help and date generated added to the description in Table 1. Syslog Server Connection info added to 3.3.1.2
0.5	2023-11-16	Iain Holness	Updates as per OCSI comments

Table of Contents

List of Tables

List of Figures

1. Introduction

The Target of Evaluation (TOE) is the Sophos Ltd. (Sophos) Sophos Firewall OS v19.0.2. The TOE is a Unified Threat Management solution with firewall and gateway functionality that runs on Sophos XGS series hardware appliances and virtual appliances. The TOE is installed on a network whenever firewall services are required.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria Evaluation Assurance Level EAL4 Evaluated Configuration. This document provides clarifications and changes to the Sophos documentation and should be used as the guiding document for the installation and administration of the TOE in the Common Criteria-evaluated configuration. The official Sophos documentation should be referred to and followed only as directed within this document.

This document is co-located with the downloadable TOE on the Sophos Licensing Portal[1]

The documents listed in Table 1 are the general Sophos Firewall OS guidance documents relevant to the use of the TOE. Table 2 lists additional documents relevant to the installation of the TOE.

Table 1 – TOE Guidance Documents

Document Name	Description	Short reference	Weblink / SHA-256 checksum
Sophos Firewall 19.0 Help	Contains detailed steps for how to properly configure and maintain the TOE. Generated on June 15, 2022.	[AdminGuide]	**URL:** https://docs.sophos.com/nsg/other/RegulatoryCompliance/files/sophosfirewall/Sophos%20Firewall%20_19.0.pdf **SHA256:** 3534013e586e269f003239674ebe2cb3050942e041c0bed8b19d65ba185719b0

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

Table 2 – Additional TOE Installation Documents

Document Name	Description	Short reference	Weblink / SHA-256 checksum
Quick Start Guide XGS 87(w)/107(w)	Includes steps for the basic initialization and setup to prepare the hardware for the TOE configuration.	[QuickstartHW][2]	**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-87-87w-107-107w.pdf **SHA256:** bb336943d44fda553205962a05337c9fdba057d0d566bcb5a5a14186aa4be8e5
Quick Start Guide XGS 116(w)/126(w)/136(w)			**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-116-116w-126-126w-136-136w.pdf **SHA256:** 5c0517a75ef31e068a5566006451d0ecf4dd71b3da980bea492b68c0a3d23c0b
Quick Start Guide XGS 2100/2300/3100/3300			**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-2100-2300-3100-3300.pdf **SHA256:** a34d3f7bad4fd638b3fb6a6e7317d5e78d7f99dc1cdbfb46a11e7d5db9900246
Quick Start Guide XGS 4300/4500			**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-4300-4500.pdf **SHA256:** 05f18dd78b78d0249b7e696c0a0c87a52fefa09cb9d78de640068c3d59e3b83a
Quick Start Guide XGS 5500/6500			**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-5500-6500.pdf **SHA256:** 55d434c39c47b02be1dab8f75f3466e34d5e2143236ce93a58b16a6413a5bc15
Quick Start Guide XGS 7500/8500			**URL:** https://docs.sophos.com/nsg/hardware/quickstart/sophos-quick-start-guide-xgs-7500-8500.pdf **SHA256:** 0a7523c2b61140baf42e507e51e4b9f0d0acde7221bf2a7c54cda6e5bd27f75f

1.2 Target Audience

The audience for this document consists of the TOE user (also referred as "Administrator" later in this document), the Sophos development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configuration

Figure 1 and Figure 2 below depict the hardware and virtual evaluated configurations of the TOE, respectively.

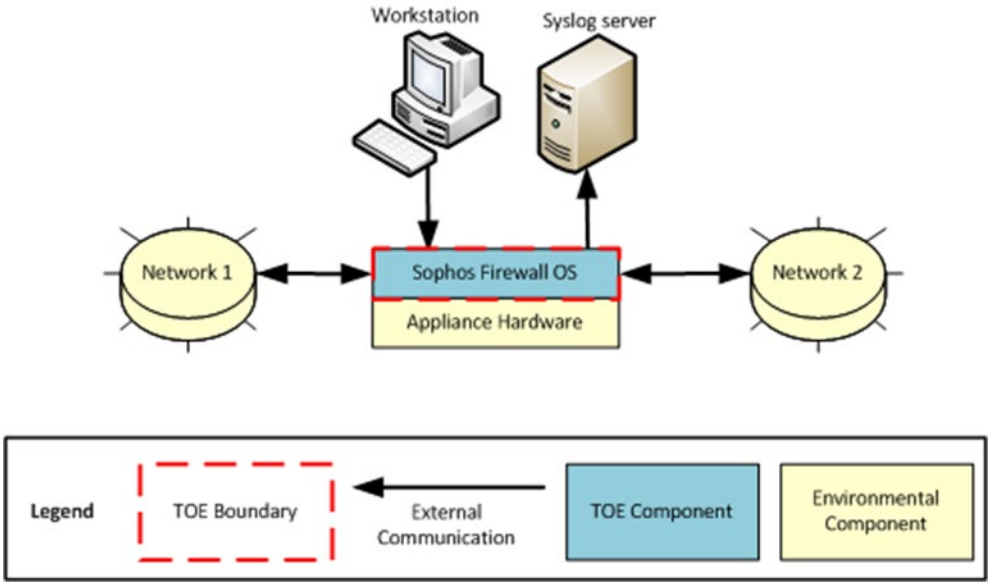

Figure 1 – Hardware Configuration of the TOE Boundary

[2] Please note that Quick Start Guides do not have explicit version numbers. They describe prerequisites on how to set up hardware appliances and are subject to occasional editorial modifications.

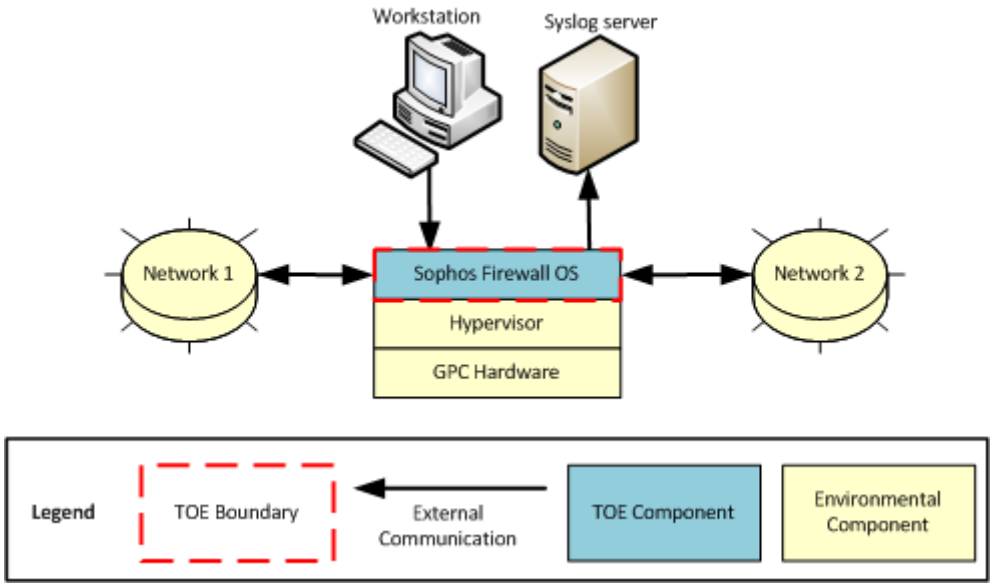

Figure 2 - Virtual Configuration of the TOE Boundary

1.4 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 3 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 3 - Assumptions

Name	Description
A.AUDIT	It is assumed that the IT environment will provide a syslog server and a means to present a readable view of the audit data.
A.GENPUR	It is assumed that the TOE will only store and execute security-relevant applications and only store data required for its secure operation.
A.NETCON	It is assumed that the TOE environment will provide the network connectivity required to allow the TOE to perform its intended function.
A.NOEVIL	It is assumed that the TOE users are non-hostile, well trained, and follow all documentation related to the TOE.
A.PHYSEC	It is assumed that the TOE is physically secure in a controlled environment and only TOE users gain physical access to the TOE.
A.SINGEN	It is assumed that information will not flow between the two networks unless it passes through the TOE.

2. Installation Procedure

This section describes the installation procedure notes and changes.

2.1 Introduction

This section describes the general installation procedures of Sophos Firewall OS hardware and virtual appliances. For the hardware and virtual installation requirements, the quick start guides are the relevant documents (see Table 2: Additional TOE Installation documents).

2.2 Secure Installation

Note: Throughout this section, the reader will be instructed to read certain passages from referenced documents. Unless otherwise stated, such instructions refer to the [AdminGuide]

2.2.1 Phase 1 – Initial Preparation

Before the administrator begins the installation, he or she must make sure that all the necessary components as listed below for the applicable configuration are in place.

Components Required for the TOE Hardware Configuration

In the TOE hardware configuration, the TOE runs on one of the 20 different models of the Sophos hardware appliances:

- XGS 87
- XGS 87w
- XGS 107
- XGS 107w
- XGS 116
- XGS 116w
- XGS 126
- XGS 126w
- XGS 136
- XGS 136w
- XGS 2100
- XGS 2300
- XGS 3100
- XGS 3300
- XGS 4300
- XGS 4500
- XGS 5500
- XGS 6500
- XGS 7500
- XGS 8500

The following components are required for the appliance installation:

- The TOE downloaded from the Sophos Licensing Portal[3] (unless prenstalled on the delivered appliance)
- This Guidance Documentation downloaded from the Licensing Portal customer portal
- The Sophos appliance and the cables supplied with it (refer to "*Before Deploying*" in Section 1 of Sophos XGS Firewall Quick Start Guide [QuickstartHW])
- A management computer – general purpose computer (GPC) with one of the following web browsers (with JavaScript enabled):
    - Mozilla Firefox v101.0 or later (recommended)
    - Google Chrome v102 or later
    - Apple Safari v15.3 or later
    - Microsoft Edge v102 or later
    - Opera v93 or later
        - For HTTPS[4]3 management sessions

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

[4] HTTPS – Hyper Text Transfer Protocol

- An external syslog server – remote computer running a syslog daemon for storing audit logs
- An uninterruptible power supply (UPS)

Components Required for the TOE Virtual Configuration (VMWare ESX/ESXI, KVM, Hyper‑V and XenApp)
In the TOE virtual configuration, the TOE runs on a virtual machine (VM) created using virtualization software installed on a GPC. The following components are required for such an installation:

- A GPC that complies with the base virtual hardware configuration defined in "*Deployment Options > Virtual"* [AdminGuide p.75]. If this minimum hardware requirement configuration is not met, the Sophos virtual appliances will go into "FAILSAFE" mode, implications of which are described in the following Sophos Knowledge Base Article (https://support.sophos.com/support/s/article/KB-000036376?language=en_US).
- VMware ESX/ESXi
    - VMware ESX/ESXi v5.0 or later installed on the GPC specified above.
    - VMware vSphere Client installed on a Windows machine to connect to the VM from the GPC.
- KVM
    - x86 machine running a recent Linux kernel on an Intel (recommended) processor with VT (virtualization technology) extensions, or an AMD processor with SVM[5] extensions (also called AMD-V).
    - Use commands given below to check if your CPU supports Intel VT or AMD‑V:
    - For Intel VT: `grep - -color vmx /proc/cpuinfo`
    - For AMD‑V: `grep - -color svm /proc/cpuinfo`
    - Install Virtual Machine Manager (virt‑manager), a desktop Graphical User Interface (GUI) application for managing Kernel Based Virtual Machines.
- Hyper‑V
    - Make sure that Microsoft Hyper -V Server 2012 R2/2016 has been installed in your network.
- XenApp
    - Make sure that XenServer has been installed in your network.
    - Install XenCenter, a desktop Graphical User Interface (GUI) application for managing XenServer.
- The TOE firmware downloaded from the "Licensing Portal[6]" customer portal.
- A management computer – GPC with one of the following web browsers (with JavaScript enabled):
    - Mozilla Firefox v101.0 or later
    - Google Chrome v102 or later
    - Apple Safari v15.3 or later
    - Microsoft Edge v102 or later
    - Opera v93 or later

  for HTTPS management sessions:
- An external syslog server – remote computer running a syslog daemon for storing audit logs
- An uninterruptable power supply (UPS)

[5] SVM – Secure Virtual Machine
[6] https://www.sophos.com/en-us/support/downloads/firewall-installers

2.2.2 Phase 2 – Installation of the TOE

This section provides the installation instructions for both the hardware and virtual configurations.

2.2.2.1 Hardware Configuration

If you are setting up the Sophos hardware appliance for the very first time (for example after a new purchase), perform the steps outlined in Sections 1 - 5 of the Sophos [QuickstartHW].[7] Then complete the initial setup as described below:

1. Connect to the firewall, which is accessible by default via `https://172.16.16.16` on port 4444. When you first connect to the firewall, you'll see the splash screen welcoming you to XGS Firewall. From here, you can choose your desired language and then click to begin.
2. The first step is to set your default administrator ('`admin`') account password. You will be provided with guidance on the minimum password requirements and whether you meet them as you type.
3. By default, the latest firmware will be automatically installed at the end of the setup process, if you have an active Internet connection at the time. It is important to deselect the check box.
4. You will need to agree to the Sophos End User License Agreement or Third-Party License and then you can click **Continue**.
5. In the next step, you can rename your firewall (by default it is the device serial number) and select your time zone.
6. Register the firewall, which requires your Licensing Portal ID and an active Internet connection.
7. Click **Continue** and you will be connected to the registration portal.
8. Here you will either need to log in using your Sophos ID credentials. You will then be asked to confirm, and the process will finish by prompting you to synchronize your license with the firewall, which can take several seconds.
9. Once the license has finished synchronizing, the basic setup process is complete, and you will see your license details displayed on the screen, including the subscriptions you purchased and their expiry dates. There is also an option to opt into the customer experience improvement program.
10. Click **Skip to Finish** to complete setting up your firewall in the main console. That way, you will be skipping the wizard, which is aimed to help you set up some the security networking essentials (e.g., network configuration (LAN[8]), on - box wireless setup, network protection features to name just a few).
11. On the login screen, log on to the Web Admin Console as '`admin`' using the password you had specified earlier.

After the initial setup, administrators must verify the version number of Sophos Firewall OS by navigating to **SYSTEM -> Backup & firmware -> Firmware** from the Web Admin Console. The firmware version that is installed is marked as "`active`".

[7] As noted above, there are various Quick Start Guides available, so please select the one that matches with your XGS appliance model.
[8] LAN – Local Area Network

If the active version is not SFOS 19.0.2 MR-2-Build472, administrators are required to install the certified version. To do so, the certified version must be downloaded from the "Licensing Portal" customer portal.[9] After clicking the **Download** button and accepting the End User License Agreement (EULA) and the export restrictions dialog, the following ISO[10] image can be downloaded:

`HW-19.0.2_MR-2-472.iso`
SHA256: `A67BD740374BA348CD4183AABCB2388FE50F58E5DE6A0E5FF2C9FF8B75188003`

After downloading the image verify the checksum of the downloaded image with the one above.

To flash the XGS appliance to the certified version that was just downloaded, the customer must burn the downloaded ISO image to a bootable USB stick. A detailed description is available in "*Reimage Sophos Firewall*" [AdminGuide p. 1806] The basic steps are repeated here for convenience:

Important note: *Re-imaging will destroy all the data on the Sophos XGS Firewall, so please ensure that a recent configuration backup has been created and saved.*

1. Burn the ISO image to a bootable USB[11] flash drive
2. Download a tool to make a bootable USB flash drive (e.g., Rufus) with downloaded image of the Firewall-OS
3. Power-off Sophos Firewall appliance
4. Optionally plug a SVGA[12] monitor to the SVGA port of your appliance. This step will help monitor the installation process. If the Sophos Firewall doesn't have an SVGA port, the installation process can be monitored using the LCD[13] panel.[14]
5. Plug the bootable USB flash drive to the USB port of the appliance
6. Power-on the Sophos Firewall appliance
7. Make sure that USB key is the first boot option in the BIOS[15]. To enter the BIOS, press the **Delete** key during the booting
8. Save and exit from the BIOS, the appliance will reboot
9. The installer starts to re-image the appliance
10. Monitor the installation progress
11. Once the firmware is installed, remove the USB flash disk and type **y** to reboot.
12. Once the installation is complete, default factory values are set on the device.

Repeat the steps outlined in Sections 1 - 5 of the Sophos [QuickstartHW].[16]You can now access the firewall, which is accessible by default via `https://172.16.16.16` on port 4444. When you first connect to the firewall, you'll see the splash screen welcoming you to XGS Firewall. From here, you can choose your desired language and then click to begin.

1. The first step is to set your default administrator ('`admin`') account password. You will be provided with guidance on the minimum password requirements and whether you meet them as you type.

[9] https://www.sophos.com/en-us/support/downloads/firewall-installers
[10] ISO – International Standards Organization
[11] USB – Universal Serial Bus
[12] SVGA – Super Video Graphics Array
[13] LCD – Liquid Crystal Display
[14] Only available for selected appliances such as XGS 2100 or higher.
[15] BIOS – Basic Input/Output System
[16] As noted above, there are various Quick Start Guides available, so please select the one that matches with your XGS appliance model.

2. By default, the latest firmware will be automatically installed at the end of the setup process, if you have an active Internet connection at the time. It is important to deselect the check box.
3. You will need to agree to the Sophos End User License Agreement or Third-Party License and then you can click **Continue**.
4. In the next step, you can rename your firewall (by default it is the device serial number) and select your time zone.
5. Register the firewall, which requires your Licensing Portal ID and an active Internet connection.
6. Click **Continue** and you will be connected to the registration portal.
7. Here you will either need to log in using your Sophos ID credentials. You will then be asked to confirm, and the process will finish by prompting you to synchronize your license with the firewall, which can take several seconds.
8. Once the license has finished synchronizing, the basic setup process is complete, and you will see your license details displayed on the screen, including the subscriptions you purchased and their expiry dates. There is also an option to opt into the customer experience improvement program.
9. Click **Skip to Finish** to complete setting up your firewall in the main console. That way, you will be skipping the wizard, which is aimed to help you set up some the security networking essentials (e.g., network configuration (LAN), on-box wireless setup, network protection features to name just a few).
10. On the login screen, log on to the Web Admin Console as '`admin`' using the password you had specified earlier.

To ensure that indeed the certified version was installed, go to **SYSTEM -> Backup & Firmware -> Firmware** and verify that SFOS 19.0.2 MR-2-Build472 is active.

2.2.2.2 Virtual Configuration example VMware ESX/ESXI

The virtual configuration is obtained by installing the TOE and Sophos XGS Firewall Virtual Appliance on a VM provided by VMware ESX/ESXi v5.0 or later. In the ESX/ESXi example there is limitation of the VMware product version which must be v5.0 or later to run the Sophos Firewall OS in the evaluated configuration. The next sections are exemplary guidelines to install the TOE on a VMware ESX/ESXi platform. The installation of the other platforms KVM, Hyper - V and XenApp are done in a similar way according to their quick start guidance and corresponding sections in [AdminGuide].

To install the Sophos XGS Firewall Virtual Appliance, first ensure that the GPC hosting the virtualized environment is configured with the minimum hardware requirements specified in [AdminGuide]. If these minimum requirements are not met, the Sophos XGS Firewall Virtual Appliance will go into “FAILSAFE” mode, the implications of which are described in the following Sophos Knowledge Base Article (https://support.sophos.com/support/s/article/KB-000036376?language=en_US).

Next, install the VMware ESX/ESXi version 5.0 or later using the installation guide links provided in [AdminGuide].

Once the hardware and VMware have been successfully installed, follow the sections entitled "Step 1" and "Step 2" under "Installation Procedure" in the [AdminGuide]. The virtual appliance ZIP file provided for the VMware ESX/ESXi 5.0 or higher platforms can be downloaded from the Licensing Portal customer portal: [17]

`VI-19.0.2_MR-2.VMW-472.zip`
SHA256: `11AAC8BA9B95C5A62D5E2E46FC66F58E84F0EC2C5C84288DD4EC9D2A4C45F030`

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

The virtual appliance ZIP files for the other platforms are available from the same download location:

`VI-19.0.2_MR-2.HYV-472.zip`
SHA256: `95D115FDDE194FE279CBCE0890B66625BDB1A04053FA44BCC3D259E5D5E02EB6`

`VI-19.0.2_MR-2.KVM-472.zip`
SHA256: `82C90A7C69EFCF6F7B63C015246554230F3117A606B7B02BFAC78A99EEAE13D2`

`VI-19.0.2_MR-2.XEN-472.zip`
SHA256: `093C0C3D3C20529A8782FA417F899EED40FB4EAF0C42E7598D7D612E7D329455`

After downloading a ZIP file, verify its checksum with the one above. After the TOE is installed and configured, follow the steps in "*Activating and registering Sophos Firewall*" [AdminGuide p. 2207] to register the virtual appliance. This is required to start up the virtual machine and bring it in a state to start the configuration of the certified version outlined in Chapter 3.

Important Note: It is preferred that a full license, purchased from Sophos, is used in the deployment of the TOE. If a trial license must be used in the deployment of the TOE, ensure that the optional "Xstream Protection Bundle" is activated in order for all features to be available.

2.2.3 Phase 3 - Evaluated Configuration of the TOE

Once the TOE is properly installed and configured as instructed above for both the appliance and virtual configurations, the following five steps are required to bring it into the evaluated configuration. All the following steps are performed with the pre-installed default administrator ('`admin`'):

1. Change the password of the default administrator ('`admin`') [AdminGuide p. 1722].
2. Configure the connection to the external syslog server [AdminGuide p. 1593] to ensure that the TOE is sending audit events to the syslog server.
3. Create firewall rules appropriate for the organization - at the time of deployment the Network Configuration Wizard that runs as part of the installation allows an administrator to choose one of three default firewall rules. These rules are at least partially based on subscription modules that are not included in the evaluated configuration of the TOE (Web filter, App filter and IPS[18] policy). Therefore, the default firewall rule selected during installation should be modified, or an additional firewall rule should be created to override it to appropriately protect the network. If no access policy is set through the Network Configuration Wizard at the time of installation, the entire traffic will be blocked.
4. Appliance access rules must be configured to ensure that no remote access to the CLI is available. This is done by selecting **SYSTEM -> Administration -> Device Access** [AdminGuide p. 1720]. Ensure that the check box in the SSH[19] column is not selected.
5. On-box reporting must be turned on to ensure that the /conf partition does not gradually fill up, resulting in the user not being able to log in to the Web GUI. This is done by accessing the TOE via SSH with an application such as PuTTY, logging in, accessing the console by entering `4` and pressing **Enter**, and running the command `set on-box-reports on`. To ensure on-box reporting has been activated, run `show on-box-reports` and make sure a "**Local Reporting : on**" message is displayed on the console.

[18] IPS - Intrusion Prevention System
[19] SSH - Secure Shell

6. Check the correct version and hotfix is installed. Using PuTTY, connect via SSH and log in with admin credentials. Enter `4` and press **Enter** to access the console. Enter the command `system diagnostics show version-info`. Ensure the **Firmware Version** displays **SFOS 19.0.2 MR-2-Build472** and the **Hotfix Tag** displays **HF050823.1.**

When using the TOE in both configurations (hardware and virtual), The TOE must be stored in a secure, access-controlled facility, with all of the administrative guidelines stated in Table 3 followed.

3. Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1. Any clarifications, exclusions, or additions are detailed here to allow the TOE Administrator to properly configure and maintain the evaluated configuration of the TOE. The TOE Administrator should have successfully completed the installation procedures listed in section 2 before applying the guidance found in sections 1.1, 3.1, and 3.3.

3.1 Clarifications

This section contains clarifications how to use the security-relevant functions and interfaces described in the operational user guidance.

3.1.1 Web Browser

The [AdminGuide] states that the latest version of Mozilla Firefox (v101 or later), Google Chrome (v102 or later), Apple Safari (v15 or later), Opera (v93 or later), Microsoft Edge (v102 or later), each with JavaScript enabled, must be used to access the Web Admin Console.

3.1.2 Login Page Options

At the Web Admin Console login page, there is the **Login** button and a language dropdown selection which offers several language options to log on to the Web Admin Console in a selected language. The **Login** fields allows an administrator to authenticate and login to their account from this page.

3.1.3 Updates

1. Go to **SYSTEM > Backup and firmware > Firmware**. Scroll down to **Latest available firmware** and click **Check for new firmware.**
2. The new firmware version shows. Click **Download** next to the version you want. Download takes a few minutes.
3. After the download is complete, click **Install**. Sophos Firewall closes all sessions and restarts with the new firmware version.

3.1.4 Setting Appliance Access

In the evaluated configuration, administrative services must be performed only through HTTPS connections to the Web Admin Console, and external authentication services must not be used. A super-administrator (With full administrative privileges) such as the default '`admin`' limits Web Admin Console access to HTTPS by navigating to the **SYSTEM -> Administration -> Device access** menu and disabling all other access options under the Admin Services category. To restrict appliance access for administrative and authentication services, refer to [AdminGuide p. 1720]

3.1.5 SSL Certificate

The Web Admin Console uses an SSL[20] certificate signed by a Certificate Authority (CA) that is not recognized by standard web browsers (e.g., Mozilla Firefox or Microsoft Edge). An administrator must download the default SSL CA certificate to the management computer at first, install it in the Trusted Certification List for the web browser being used, and install it in the Trusted Root Authority Container for the management computer.

The TOE offers the default SSL CA certificate to be downloaded in the form of a compressed .zip file that contains the following files

- `default.pem`
- `default.der`

The filename is a combination of the name of the CA and file extension, `pem`[21] and `der`[22], respectively. These files are used for the client-side of the SSL connection, which is outside of the scope of this evaluation. The following paragraphs describe how to install certificates to the various supported web browsers:

Microsoft Edge

1. Click on the three dots on the top right of the browser window. In the dropdown menu, click **Settings.**
2. Click on **Privacy, search, and services.** Scroll down to **Security** and click on **Manage certificates.**
3. In the popup window, click the **Import** button to start the Certificate Import Wizard.
4. Import the Certificate downloaded as described in the first paragraph of 3.1.5 using this wizard.

Firefox

1. In the Menu Bar, click **Tools -> Options** to display the Options window.
2. Switch to the Advanced tab and then select the Certificates tab.
3. Click **View Certificate** to display the Certificate Manager window.
4. Switch to the Authorities tab and click **Import**.
5. Select the Certificate downloaded as described in the first paragraph of 3.1.5, click **Open**.
6. In the Downloading Certificate window, select **Trust this CA** to identify websites and click OK.

Google Chrome

1. To the right of the Address Bar, click on **Customize and control Google Chrome** button and click **Settings**.
2. Click **Show advanced settings** and scroll down to HTTPS/SSL.
3. Click **Manage Certificates...** to display the Certificates window.
4. Switch to the Trusted Root Certification Authorities tab and click the **Import** button to start the Certificate Import Wizard.
5. Import the Certificate downloaded as described in the first paragraph of 3.1.5 using this wizard.

[20] SSL - Secure Socket Layer
[21] The PEM extension is used for different types of X.509 files which contain ASCII (Base64) armored data.
[22] The DER extension is used for binary DER encoded certificates.

Safari

1. Download the SSL CA Certificate as described in the first paragraph of 3.1.5.
2. Once downloaded, double-click the Certificate. This launches Keychain Access and displays a Certificate Not Trusted warning.
3. Click **Always Trust** to import the certificate into the Login Keychain.

Opera

1. Click the **Opera** button on the top left corner of the screen and click **Settings**.
2. Switch to the Privacy & Security tab.
3. Under HTTPS/SSL, click **Manage Certificates…** to display the Certificates window.
4. Switch to the Trusted Root Certification Authorities tab and click the **Import** button to start the Certificate Import Wizard.
5. Import the Certificate downloaded as described in the first paragraph of 3.1.5 using this wizard.

Install the Certificate in the local machines Trusted Root Authority container as follows:

Windows

1. Open the Microsoft Management Console by typing "`MMC`" in the "Run" box.
2. Open the Add or Remove Snap-in by selecting **FILE -> ADD/REMOVE SNAP-IN...**
3. Select Certificates from the list and click **Add** to display the Certificates Snap-in window.
4. Select the Computer Account and click **Next**.
5. Click **Finish** and close the list of snap-ins.
6. Click **OK** to add the certificates snap-in, which should now be visible in the Add/Remove Snap-ins window.
7. Expand the list of certificate containers, right click **Trusted Root Authorities**, and choose **All Tasks -> Import** to start Certificate Import Wizard.
8. Import the Certificate downloaded as described in the first paragraph of 3.1.5 using this wizard.

Mac OS

1. Download the SSL CA Certificate as described in the first paragraph of 3.1.5.
2. Once downloaded, double-click the Certificate. This launches Keychain Access and displays a Certificate Not Trusted warning.
3. Click **Always Trust** to import the certificate into Login Keychain.

3.1.6 Changing Passwords

The TOE comes with one default super administrator account ('`admin`') pre-installed who has full privileges to the entire TOE security functionality. It is recommended to change this administrator's password immediately after installation of the TOE. This is done by navigating to **SYSTEM -> Administration -> Device Access** in the Web Admin Console [AdminGuide p. 1720]. The TOE also allows password complexity settings [AdminGuide p. 1732]. For the evaluated configuration, enable the 'Password Complexity Check' in the **SYSTEM -> Administration -> Admin and user settings** menu and ensure that passwords are at least 8 characters long.

3.1.7 Administrator Profiles

The TOE comes with five different administrator profiles installed:

- Security Admin: As a Security Admin, you have read/write privileges to all functions of the TOE, excluding device access, and logs and reports.
- Administrator: As an Administrator, you have full access privileges to all functions of the TOE.
- Audit Admin: As an Audit Admin, you have only read/write privileges to various log and reports related functions of the TOE.
- Crypto Admin: As a Crypto Admin, you only have read/write privileges for the configuration of security certificates.
    - **NOTE:** *This profile is excluded from this evaluation*
- HA Profile: As someone assigned with the HA Profile, you have only read privileges to all functions of the TOE
    - **NOTE**: *This profile is excluded from this evaluation.*

3.1.8 User Interfaces

The TOE provides the Web Admin Console to perform all security functionality of the TOE. The Web Admin Console has full access to and control of the TOE.

The TOE additionally contains the Network Traffic In Interface, which is responsible for applying the Traffic Information Flow Control SFP to the traffic transmitted through this interface. This process happens transparently, and users have no way to manipulate the TOE through this interface. Additionally, no management can be performed through this interface.

3.1.9 TOE Modes of Operation

Though not specified in the TOE user guidance, it should be understood that the TOE has only one mode of operation.

3.1.10 HTTPS Port Number Login Authentication

To maintain security after a configuration change, administrators must take the following actions when changing the Web Console port number:

1. Close the browser after the Web Console port number is altered
2. Re-open the browser
3. Navigate back to https://<TOE IP>:<Port Number>, where Port Number is the port number that the user has just changed within the Web Console
4. The login screen is displayed, requiring reauthentication to access the TOE

If the browser is not closed, navigating to the Web Console with the new port number in the URL does not require reauthentication. Users must close the browser to allow for reauthentication into the TOE.

3.2 Exclusions

As stated in the Security Target (ST), the following product features and functionality are excluded from the TOE, are not part of the evaluated configuration of the TOE and should not be operational. During runtime an administrator must not use these features to ensure that the TOE is operating in the evaluated configuration:

- Use of the Command Line Interface (CLI)
- Use of the User Portal
- Use of the HAProfile and Crypto Admin profiles
- Creation of new Administrator-type profiles
- Use of the SNMP[23] functionality
- Use of the external authentication functionality
- Use of the VPN[24] functionality
- Use of the intrusion prevention system functionality
- Use of the gateway antivirus/antispyware functionality
- Use of the gateway antispam functionality
- Use of the outbound spam protection functionality
- Use of the web filtering functionality
- Use of the secure syslog functionality
- Use of the log suppression functionality
- Use of the Web Portal login CAPTCHA functionality
- Upgrading from previous TOE firmware versions

3.3 Additions

This section contains additional guidance that was not described in the operational user guidance.

3.3.1 Additional Configurations

3.3.1.1 Additional Message

An Administrator must enable the advisory message before entering the evaluated configuration. This can be done in the Web Admin Console by navigating to the **SYSTEM -> Administration -> Admin and user settings** menu option and clicking the box next to **Enable Login Disclaimer** [AdminGuide p. 1732].

3.3.1.2 Audit Configuration

Detailed log information and reports are available locally through the Web Admin Console until a system shutdown for analysis of current network activity. Audit events that precede a system power loss can only be viewed on the external syslog server. This includes the audit record of the shutdown of the audit function. Therefore, an external syslog server is required in the evaluated configuration to provide historical analysis of network activity to help identify security issues and reduce network abuse. The administrator or Audit Admin must configure auditing [AdminGuide p. 1870] to enable the syslog server and choose the appropriate log settings. For the evaluated configuration, the following log settings must be enabled:

- Firewall (Firewall and invalid Traffic)

[23] SNMP – Simple Network Management Protocol
[24] VPN – Virtual Private Network

- Events (all options)

If the connection between the TOE and the external syslog server is lost, any audit logs output during that outage are lost.

3.3.1.3 DoS & Spoof Prevention

The TOE must be configured to enable the DoS[25] & Spoof Prevention. This is required to ensure that the TOE remains operable in case of a denial-of-service attack. Go to **PROTECT -> Intrusion Prevention -> DoS & Spoof Protection -> DoS settings** and enter the packet rates consistent with your organizational security policy. [AdminGuide p. 403].

3.3.2 Reporting product Flaws

Administrators report flaws through any of the following ways:

- Web support after logging into the customer support portal (**URL**: https://support.sophos.com/support/s/?language=en_US#t=AllTab&sort=relevancy)
- Phone support, by calling a Customer Support representative (regional toll-free numbers are available)
- Live online chat, accessed via customer support after submitting credentials

Administrators who report a security flaw are provided with a confirmation that the case was created according to their service level agreement. Status updates are sent to the case owner by the Support Team. Subsequent updates are sent in a cadence determined by the severity and/or support level until an estimated time for a fix or an actual resolution is available. Case owners can inquire about the status of a reported security flaws through the very same procedures listed above.

After a flaw is resolved, Sophos' support team members update the support ticket to indicate the release in which the issue will be resolved and assigns the ticket to the assigned support team member. The support team member notifies the customer of the resolution and closes the ticket. The support team member uses the information from the comments field of internal Jira tickets (not customer-facing) to provide flaw remediation information to the customer. The fix is made available to all customers in the next release or a future release. Customers are notified of new releases through the Sophos Web Admin Console. Customers may then go to the customer download page to retrieve the update and its associated checksum. If necessary, the information from the comments field of Jira will be included in the release notes for security flaws (available from the Sophos Knowledgebase [26]).

3.3.3 Security Relevant Events

The following security relevant events must be taken into consideration to maintain the security functionality of the TOE.

Table 4 - Security Relevant Events

Security relevant Event	Action
Shutdown of the TOE because of manipulation of the audit trail is suspected	The admin must investigate if there is a manipulation of the audit trail in the logs (e.g., logs were deleted).
Critical shutdown because of a power loss	The Audit Admin must check after reboot that the audit trail is still valid by checking in the Log Viewer if there was an emergency event logged and logging is still running

[25] DoS - Denial-of-Service
[26] https://community.sophos.com/sophos-xg-firewall/b/blog

Security relevant Event	Action
The TOE is in an unidentified state	An Admin must check if the TOE is in a certified state according to this guidance by comparing the version number in the Licensing Portal with the one installed on the appliance. The admin must further check if the excluded features mentioned in Section 3.2 are disabled.
The TOE and its security features maybe compromised	An Admin must check the logs in the log viewer. If the suspicion cannot be resolved, the TOE must be initialized from the scratch as described in Section 2.2.
The TOE is not operating correctly	Follow the troubleshooting guidelines [AdminGuide p.948] and operations in the Web Admin Console in the **MONITOR & ANALYZE -> Diagnostics** menu.

3.3.4 Troubleshooting

3.3.4.1 UTF-8 Character in Backup File

When a UTF-8[27] character is present in the backup file name, an issue arises where the user is unable to download the backup file. To resolve this, remove the UTF-8 character from the backup file and the user will be able to download the backup file normally.

3.3.4.2 /conf File Filling Up

If the On-box reports of the appliance is turned off or disabled, the /conf file gradually fills up. When the conf partition gets to 100%, the user is unable to login. To resolve this, if the On-box reports are turned off, turn on the On-box reporting from the console by navigating to the console and entering `set on-box-reports on`.

[27] UTF-8 – Unicode Transformation Format-8

4. Acronyms and Terms

This section defines the acronyms and terms used throughout this document.

Table 5 - Acronyms

Acronym	Definition
TOE	Target of Evaluation
BIOS	Basic Input/Output System
CA	Certificate Authority
CLI	Command Line Interface
DoS	Denial-of-Service
EAL	Evaluation Assurance Level
GPC	General Purpose Computer
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention System
ISO	International Standards Organization
LAN	Local Area Network
LCD	Liquid Crystal Display
OS	Operating System
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
ST	Security Target
SVGA	Super Video Graphics Array
SVM	Secure Virtual Machine
UPS	Uninterrupted Power Supply
USB	Universal Serial Bus
VM	Virtual Machine
VT	Virtualization Technology
VPN	Virtual Private Network

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com