

# CIS Sophos Firewall v22 Benchmark

v1.0.0 - 03-25-2026

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

For information on referencing and/or citing CIS Benchmarks in 3<sup>rd</sup> party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal ([legalnotices@cisecurity.org](mailto:legalnotices@cisecurity.org)) and request guidance on copyright usage.

**NOTE:** It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3<sup>rd</sup> party (non-CIS owned) site.

# Table of Contents

|                                                                                                                   |           |
|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Terms of Use .....</b>                                                                                         | <b>1</b>  |
| <b>Table of Contents .....</b>                                                                                    | <b>2</b>  |
| <b>Overview .....</b>                                                                                             | <b>5</b>  |
| <b>Important Usage Information .....</b>                                                                          | <b>5</b>  |
| Key Stakeholders .....                                                                                            | 5         |
| Apply the Correct Version of a Benchmark .....                                                                    | 6         |
| Exceptions .....                                                                                                  | 6         |
| Remediation .....                                                                                                 | 7         |
| Summary .....                                                                                                     | 7         |
| <b>Target Technology Details .....</b>                                                                            | <b>8</b>  |
| <b>Intended Audience.....</b>                                                                                     | <b>8</b>  |
| <b>Consensus Guidance .....</b>                                                                                   | <b>9</b>  |
| <b>Typographical Conventions.....</b>                                                                             | <b>10</b> |
| <b>Recommendation Definitions.....</b>                                                                            | <b>11</b> |
| Title.....                                                                                                        | 11        |
| <b>Assessment Status.....</b>                                                                                     | <b>11</b> |
| Automated .....                                                                                                   | 11        |
| Manual.....                                                                                                       | 11        |
| Profile .....                                                                                                     | 11        |
| Description.....                                                                                                  | 11        |
| Rationale Statement .....                                                                                         | 11        |
| Impact Statement.....                                                                                             | 12        |
| Audit Procedure.....                                                                                              | 12        |
| Remediation Procedure.....                                                                                        | 12        |
| Default Value.....                                                                                                | 12        |
| References .....                                                                                                  | 12        |
| CIS Critical Security Controls® (CIS Controls®).....                                                              | 12        |
| Additional Information.....                                                                                       | 12        |
| Profile Definitions .....                                                                                         | 13        |
| Acknowledgements .....                                                                                            | 14        |
| <b>Recommendations .....</b>                                                                                      | <b>15</b> |
| <b>1 Device Setup And Administration .....</b>                                                                    | <b>15</b> |
| <b>1.1 General Settings .....</b>                                                                                 | <b>16</b> |
| 1.1.1 Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in (Automated) ..... | 17        |
| 1.1.2 Ensure login disclaimer is set (Automated) .....                                                            | 20        |

|                                                                                                                                                                          |           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 1.1.3 Ensure NTP servers are configured appropriately (Manual) .....                                                                                                     | 22        |
| 1.1.4 Ensure SSL server certificate for remote SSL VPN is configured correctly (Manual) .....                                                                            | 24        |
| 1.1.5 Ensure password complexity check is enabled (Automated) .....                                                                                                      | 26        |
| 1.1.6 Ensure management access to the device is restricted from selected IP addresses and<br>disable from WAN Zone (Manual) .....                                        | 29        |
| 1.1.7 Ensure valid certificate is set for web browser used to access Webadmin interface<br>(Manual) .....                                                                | 32        |
| 1.1.8 Ensure MFA for Web console access and remote access VPN (Manual) .....                                                                                             | 35        |
| 1.1.9 Ensure MFA for default admin (Manual) .....                                                                                                                        | 37        |
| 1.1.10 Set Hostname (Automated) .....                                                                                                                                    | 38        |
| <b>1.2 SNMP &amp; Device Notification Settings .....</b>                                                                                                                 | <b>40</b> |
| 1.2.1 Ensure SNMPv3 is selected for queries and traps (Automated) .....                                                                                                  | 41        |
| 1.2.2 Ensure notification is configured to send system and security events (Manual) .....                                                                                | 43        |
| <b>2 User Identification &amp; Authentication .....</b>                                                                                                                  | <b>46</b> |
| 2.1 Ensure Firewall rules are configured to identify users before authorizing access (Manual)<br>.....                                                                   | 47        |
| 2.2 Ensure Encrypted connection is used in connecting external Active Directory and LDAP<br>(Manual) .....                                                               | 50        |
| <b>3 System Services, Firmware and Updates .....</b>                                                                                                                     | <b>52</b> |
| 3.1 Ensure "Fully Synchronized" High Availability peer is configured (Manual) .....                                                                                      | 53        |
| 3.2 Ensure 'Pattern updates' is set to download and install updates every 15 minutes<br>(Automated) .....                                                                | 56        |
| 3.3 Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes' (Manual) .....                                                                                  | 59        |
| 3.4 Ensure Sophos Firewall takes encrypted backup of the configuration and send to<br>designated email address with scheduled frequency (Manual) .....                   | 61        |
| 3.5 Ensure No Expired Subscription Licenses (Manual) .....                                                                                                               | 64        |
| 3.6 Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode" (Manual) .....                                                                                | 66        |
| 3.7 Ensure Logging is enabled on firewall rules and configured to send logs to the external<br>syslog server (Manual) .....                                              | 68        |
| <b>4 Advanced Threat &amp; Synchronized Security .....</b>                                                                                                               | <b>72</b> |
| 4.1 Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and<br>Policy is set to 'Log and drop' (Manual) .....                            | 73        |
| 4.2 Ensure Zero-day protection is enabled at the firewall rule for web protection and does not<br>exclude any file type from zero-day protection analysis (Manual) ..... | 76        |
| 4.3 Ensure Zero-day protection is enabled for Email Protection and set to MTA mode (Manual)<br>.....                                                                     | 79        |
| 4.4 Ensure Synchronized Security Heartbeat is enforced on Firewall Rules (Manual) .....                                                                                  | 82        |
| 4.5 Ensure MDR Threat Feeds is enabled (Manual) .....                                                                                                                    | 85        |
| 4.6 Ensure Third-party Threat Feeds is enabled (Manual) .....                                                                                                            | 87        |
| 4.7 Ensure NDR Essentials is enabled and configured (Manual) .....                                                                                                       | 90        |
| <b>5 Protection Rules And Profiles .....</b>                                                                                                                             | <b>92</b> |
| 5.1 Ensure Web Policy is configured to block inappropriate URLs, Malware and content<br>scanning is configured correctly. (Manual) .....                                 | 93        |
| 5.2 Ensure SSL/TLS inspection rules is enabled to all relevant firewall policies (Manual) .....                                                                          | 96        |
| 5.3 Ensure Application filter is set to block high risk (Risk Level 4 and 5) applications (Manual)<br>.....                                                              | 99        |
| 5.4 Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules (Manual) .                                                                            | 101       |
| 5.5 Ensure Web Application Firewall (WAF) is configured with appropriate protection policies<br>in all the WAF rules in use (Manual) .....                               | 104       |
| 5.6 Ensure Email protection is configured with appropriate protection policies (Manual) .....                                                                            | 109       |
| 5.7 Ensure DoS & Spoof Protection is enabled with the appropriate settings (Manual) .....                                                                                | 113       |
| 5.8 Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should<br>not be directly accessible from WAN Zone (Manual) .....                       | 115       |

|                                                                                                                       |            |
|-----------------------------------------------------------------------------------------------------------------------|------------|
| 5.9 Ensure Wireless Protection is configured with secure configuration (Manual) .....                                 | 117        |
| 5.10 Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from<br>`WAN` Zone (Manual)..... | 120        |
| 5.11 Ensure a Optimal Firewall health check score (Manual) .....                                                      | 122        |
| 5.12 Ensure Sophos DNS protection is configured (Manual).....                                                         | 123        |
| <b>Appendix: Summary Table .....</b>                                                                                  | <b>126</b> |
| <b>Appendix: CIS Controls v7 IG 1 Mapped Recommendations .....</b>                                                    | <b>130</b> |
| <b>Appendix: CIS Controls v7 IG 2 Mapped Recommendations .....</b>                                                    | <b>131</b> |
| <b>Appendix: CIS Controls v7 IG 3 Mapped Recommendations .....</b>                                                    | <b>133</b> |
| <b>Appendix: CIS Controls v7 Unmapped Recommendations.....</b>                                                        | <b>135</b> |
| <b>Appendix: CIS Controls v8 IG 1 Mapped Recommendations .....</b>                                                    | <b>136</b> |
| <b>Appendix: CIS Controls v8 IG 2 Mapped Recommendations .....</b>                                                    | <b>138</b> |
| <b>Appendix: CIS Controls v8 IG 3 Mapped Recommendations .....</b>                                                    | <b>140</b> |
| <b>Appendix: CIS Controls v8 Unmapped Recommendations.....</b>                                                        | <b>142</b> |
| <b>Appendix: Change History .....</b>                                                                                 | <b>143</b> |

# Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

## Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

**NOTE:** Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

## Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

## Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

## Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

## Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

**When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.**

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

## Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

**NOTE:** As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.



## Target Technology Details

**Overview** This document provides prescriptive guidance for establishing a secure configuration posture for Sophos Firewalls running SFOS version v22. This guide was tested against SFOS v22. To obtain the latest version of this guide, please visit <http://benchmarks.cisecurity.org>. If you have questions, comments, or have identified ways to improve this guide, please write us at [feedback@cisecurity.org](mailto:feedback@cisecurity.org).

## Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate SFOS v22 on a Sophos Firewall.

## Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention                                      | Meaning                                                                                                                                                           |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>Stylized Monospace font</code>            | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.                                                           |
| <code>Monospace font</code>                     | Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.                                                  |
| <code>&lt;Monospace font in brackets&gt;</code> | Text set in angle brackets denote a variable requiring substitution for a real value.                                                                             |
| <i>Italic font</i>                              | Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.  |
| <b>Bold font</b>                                | Additional information or caveats things like <b>Notes</b> , <b>Warnings</b> , or <b>Cautions</b> (usually just the word itself and the rest of the text normal). |

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation.

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to: o be practical and prudent; o provide a clear security benefit; and o not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics: o are intended for environments or use cases where security is paramount o acts as a defense in depth measure o may negatively inhibit the utility or performance of the technology.

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

### **Contributor**

Jayesh Panicker

Priyanka Yadav

Darren Stevenson

# Recommendations

## 1 Device Setup And Administration

The Device Setup section covers requirements for login banners, logging, management interfaces, password strength, device management authentication, SNMP polling, notifications and device services.



## **1.1 General Settings**

The General settings section includes banner, device access profiles and logging settings.

### *1.1.1 Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

Set to automatically sign out the administrator from the web admin console after the configured time of inactivity. (Default: 10 minutes)

Set to block sign-in to the web admin console and CLI after the maximum numbers of failed sign-in attempts and the duration (in seconds) which attempts can be made from a single IP address.

#### **Rationale:**

An unattended computer with an open administrative session to the device could allow an unauthorized user access to the firewall's management interface. Thwart brute force attempts against login sessions to block multiple sign-in failures.

## Audit:

Navigate to `System > Administration > Admin and user settings > Login security`

Verify that `Logout admin session after \_ Minutes of inactivity` is checked and configured with no more than 10 minutes of default value.

Verify that `Block login` is checked.

Verify that `After \_ unsuccessful attempts from same IP in \_\_ Seconds (1-120)` is configured with values of 5 and 60 respectively.

Verify that `Block login access for \_\_ minutes [1-60]` is set to at least 5.

## Remediation:

Navigate to `System > Administration > Admin and user settings > Login security`.

Set `Logout admin session after \_ Minutes of inactivity` is checked and configured with no more than 10 minutes of default value.

Set `Block login` is checked.

Set `After \_ unsuccessful attempts from same IP in \_\_ Seconds (1-120)` is configured with values of 5 and 60 respectively.

Set `Block login access for \_\_ minutes [1-60]` to at least 5

## Default Value:

Not Enabled: Log out admin session after 10 minutes. Enabled: Block Login

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/AdminSettings/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                       | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u></b><br>Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes. |  |  |  |

| Controls Version | Control                                                                                                                                   | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v7               | <b>16.11 Lock Workstation Sessions After Inactivity</b><br>Automatically lock workstation sessions after a standard period of inactivity. |  |  |  |

## 1.1.2 Ensure login disclaimer is set (Automated)

### Profile Applicability:

- Level 1

### Description:

Configure a login disclaimer, ideally approved by the organization's legal team. This banner should at minimum prohibit unauthorized access, provide notice of logging or monitoring, and avoid using the word "welcome" or similar words of invitation.

### Rationale:

Through a properly stated login banner, the risk of unintentional access to the device by unauthorized users is reduced. Should legal action take place against a person accessing the device without authorization, the login banner greatly diminishes a defendant's claim of ignorance.

### Audit:

```
Navigate to `System > Administration > Admin and User Settings > Login  
Disclaimer Settings`.  
Verify `Enable login disclaimer` is checked and disclaimer message is set  
appropriately.
```

### Remediation:

```
Navigate to `System > Administration > Admin and User Settings > Login  
Disclaimer Settings`.  
`Enable login disclaimer` is checked and set the disclaimer message  
appropriately.
```

### Default Value:

Not Configured

### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/AdminSettings/index.html>

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 1.1.3 Ensure NTP servers are configured appropriately (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Synchronize the clock on Sophos firewall with NTP servers.

#### Rationale:

NTP enables the device to maintain an accurate time and date when receiving updates from a reliable NTP server. Accurate timestamps are critical when correlating events with other systems, troubleshooting, or performing investigative work. Logs and certain cryptographic functions, such as those utilizing certificates, rely on accurate time and date parameters. In addition, rules referencing a Schedule object will not function as intended if the device's time and date are incorrect.

#### Audit:

Navigate to `System > Administration > Time`.

Verify that `Time Zone` is set correctly.

Verify that `Use pre-defined NTP Server` Or `Use custom NTP Server` is checked and synchronize the device's clock.

#### Remediation:

Navigate to `System > Administration > Time`.

Set `Time Zone` correctly.

Set `Use pre-defined NTP Server` Or `Use custom NTP Server` is checked and synchronize the device's clock.

#### Default Value:

Not configured

#### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/AdministrationTimeSet/index.html>

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                                                      | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.4 <u>Standardize Time Synchronization</u></b><br>Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.                                                          |      |  |  |
| v7               | <b>6.1 <u>Utilize Three Synchronized Time Sources</u></b><br>Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent. |      |  |  |



### *1.1.4 Ensure SSL server certificate for remote SSL VPN is configured correctly (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

The Certificate used to secure SSL VPN should satisfy the following criteria.

- It should be a valid certificate from a trusted source. In most cases this means a trusted Public Certificate Authority as remote sslvpn users may not have access to any Private Certificate Authorities for Certificate validation.
- The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
- The key length used to encrypt the certificate should be 2048 bits or more.
- The hash used to sign the certificate should be SHA-2 or better.

#### **Rationale:**

If presented with a certificate error, the end user in most cases will not be able to tell if their session is using a self-signed or expired certificate, or if their session is being eavesdropped on or injected into by a "Man in the Middle" attack.

#### **Impact:**

Not using a trusted Certificate, issued by a trusted Public Certificate Authority means that clients establishing VPN sessions will always see an error indicating an untrusted Certificate. This means that they will have no method of validating if their VPN session is being hijacked by a "Man in the Middle" (MitM) attack. It also "trains" them to bypass certificate warnings for other services, making MitM attacks easier for those other services as well.

## Audit:

Verify that the certificate being used to secure the SSL VPN meets the criteria listed.

Navigate to `System > Administration > Admin and User settings > Admin console and end-user interaction > Certificate`

Ensure that a valid certificate is applied to the User portal.

Navigate to `Configure > Remote Access VPN > SSL VPN > SSL VPN global settings > SSL server certificate`.

Ensure that a valid certificate is used for the SSL VPN Gateway.

## Remediation:

Create a CSR and install a certificate from a public CA.

Navigate to `System > Administration > Admin and User settings > Admin console and end-user interaction > Certificate`.

Set a valid certificate to the User portal.

Navigate to `Configure > Remote Access VPN > SSL VPN > SSL VPN global settings > SSL server certificate`.

Set a valid certificate for the SSL VPN Gateway.

## Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RemoteAccessVPN/IPsecSSL/SSLVPN/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                         | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |      |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                |      |  |  |

### *1.1.5 Ensure password complexity check is enabled (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

This checks all new passwords to ensure that they meet basic requirements for strong passwords. CIS Password Recommendations:

- Length: 14+ characters for password-only, 8+ for MFA.
- Composition: Allow all character types; require at least one non-alphabetic, one uppercase, one lowercase and one numeric characters for password-only accounts.
- Passphrases: Use multiple words for memorability (e.g., "Th3F0rdMust@ngis#1").
- Expiration: Change immediately on compromise; annual change as a "backstop".
- Banning: Check against common, weak, or previously used passwords.
- MFA: Implement wherever possible; it significantly lowers complexity requirements.

#### **Rationale:**

Password complexity recommendations are derived from the USGCB (United States Government Configuration Baseline), Common Weakness Enumeration, and benchmarks published by the CIS (Center for Internet Security). Password complexity adds entropy to a password, in comparison to a simple password of the same length. A complex password is more difficult to attack, either directly against administrative interfaces or cryptographically, against captured password hashes. However, making a password of greater length will generally have a greater impact in this regard, in comparison to making a shorter password more complex.

#### **Impact:**

Simple passwords make an attacker's job very easy. There is a reasonably short list of commonly used admin passwords for network infrastructure, not enforcing password lengths and complexity can lend itself to making an attacker's brute force attack successful.

## Audit:

Navigate to `System > Administration > Admin and user settings > Administrator password complexity settings > Enable password complexity check`.

Verify that `Enable password complexity check` is enabled.

Ensure that the various password settings to values that are appropriate to your organization. Should be checked for use at least one uppercase and one lowercase letter, include at least 1 numeric character and include at least 1 special character like @,\$,!,etc.

## Remediation:

Navigate to `System > Administration > Admin and user settings > Administrator password complexity settings > Enable password complexity check`.

Set Enable password complexity check.

Set that the various password settings to values that are appropriate to your organization. It is suggested that there at least be some special characters enforced, and that a minimum length be set. Ensure that Minimum Uppercase, Lowercase and Special Characters.

Operationally, dictionary words should be avoided for all passwords - passphrases are a much better alternative.

## Default Value:

Enabled

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/AdminSettings/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                   | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.7 <u>Manage Default Accounts on Enterprise Assets and Software</u></b><br>Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable. |  |  |  |

| Controls Version | Control                                                                                                                                                           | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v7               | <b>4.2 Change Default Passwords</b><br>Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts. |  |  |  |

### *1.1.6 Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone (Manual)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

It is recommended to limit exposure of Firewall administration services from WAN/untrusted zone. When necessary, leverage on remote VPN or limiting only from selected IP addresses, or use of Sophos Central for firewall administration.

For additional security control - RBAC and administrative accounts can be enabled with 2-factor authentication using built-in RADIUS Server.

By disabling 'HTTPS', 'SSH' and 'Network services (PING/PING6, DNS, SMTP RELAY, SNMP)' on WAN zone to protect against reconnaissance attempts, network scanners and potential adversary.

#### **Rationale:**

When the device is exposed to the internet with service ports, it could be subjected to DOS, brute-force attempts, and underlying vulnerability on service ports can be discovered by the attacker.

#### **Impact:**

When left enabled - it could lead to brute force attempt on the Webadmin interface, denial of service attack from wide range of IP addresses and increase attack surface from potential adversary.

## Audit:

Navigate to `System > Administration > Device Access > Local service ACL`.

Verify `HTTPS, SSH, PING/PING6, DNS, SMTP RELAY, SNMP` on `WAN Zone` is unchecked.

Navigate to `Local service ACL exception rule`.

Verify that `Added exception rule` only allows limited IP addresses for device management.

## Remediation:

Navigate to `System > Administration > Device Access > Local service ACL`.

Uncheck `HTTPS, SSH, PING/PING6, DNS, SMTP RELAY, SNMP` on `WAN Zone`.

## Default Value:

Above services are disabled by default on WAN zone

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.htm>  
!

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                             | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                                                                                                                      | ●    | ●    | ●    |
| v8               | <b>12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u></b><br>Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access. |      |      | ●    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                                                                                                                       | ●    | ●    | ●    |

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                              | IG 1 | IG 2 | IG 3 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v7               | <p><b>11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u></b></p> <p>Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.</p> |      | ●    | ●    |



### *1.1.7 Ensure valid certificate is set for web browser used to access Webadmin interface (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Default HTTPS port 4444 is used to access Sophos Firewall's Webadmin interface. HTTPS certificate used to secure the administrative session should satisfy the following criteria:

1. A valid certificate from a trusted source should be used. While a certificate from a trusted Public Certificate Authority is certainly valid, one from a trusted Private Certificate Authority is absolutely acceptable for this purpose.
2. The certificate should have a valid date. It should not have a "to" date in the past (it should not be expired), and should not have a "from" date in the future.
3. The certificate should use an acceptable cipher and encryption level.

#### **Rationale:**

If a certificate that is self-signed, expired, or otherwise invalid is used for HTTPS interface, administrators in most cases will not be able to tell if their session is being eavesdropped or injected into by "Man in the Middle" attack.

#### **Impact:**

If the default self-signed certificate is used, an administrator will not be able to tell if their HTTPS session is being hijacked or not. Using a trusted certificate ensures that the session is both encrypted and trusted.

## Audit:

Navigate to `System > Certificates > Certificates`.

Verify that the certificate used to secure HTTPS sessions meets the criteria by reviewing the appropriate certificate.

Navigate to `System > Administration > Admin settings > Admin console and end-user interaction > Certificate`.

Verify that correct Certificate is used for Webadmin, user portal, captive portal and SPX reply portal.

## Remediation:

If a new administrative Certificate is needed, acquire a Certificate that meets the stated criteria and upload it to the Sophos Firewall. Optionally, download the appliance Certificate Authority to the web browser used for administration.

Navigate to `System > Certificates > Certificates > Add`

Import an appropriate Certificate for your administrative session, from a trusted Certificate Authority.

Navigate to `System > Administration > Admin settings > Admin console and end-user interaction > Certificate`

Choose the correct certificate to use for the web based administrative session.

## Default Value:

A self-signed certificate is used by default for the administrative interface.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/AdminSettings/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Certificates/Certificates/index.html>

## Additional Information:

Verify that the clock is both accurate and reliable on the Sophos Firewall and on the administrative workstations before setting the SSL/TLS Service Profile. Inaccurate or mismatched clocks will result in certificate errors and can result in loss of HTTPS administrative access.

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                              | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                      |                                                                                     |  |  |
| v8               | <b>6.5 <u>Require MFA for Administrative Access</u></b><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider. |  |  |  |
| v7               | <b>4.5 <u>Use Multifactor Authentication For All Administrative Access</u></b><br>Use multi-factor authentication and encrypted channels for all administrative account access.                                      |                                                                                     |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                     |                                                                                     |  |  |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.      |                                                                                     |  |  |

### *1.1.8 Ensure MFA for Web console access and remote access VPN (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

MFA adds an extra layer of security to the firewall's web console access. Enforcing MFA significantly reduces the risk of unauthorized configuration changes to the firewall. Similarly, enforcing MFA for the VPN connections adds an additional verification factor beyond passwords, ensuring that only verified users can establish a VPN session

**Rationale:**

Firewall web console provides high-privileged access, so enforcing MFA reduces the risk of unauthorized configuration changes and any harmful changes to the critical network security policies. By enforcing strong validation at the VPN entry point, MFA reduces the likelihood of attackers gaining a foothold and moving deeper into the environment.

## Audit:

Navigate to ' Configure ' > 'Authentication' > 'Multi-factor authentication' > 'Multi-factor authentication settings'

Select ' Specific Users and groups ' > ' Add the user or group '

Enable ' Generate OTP toles with next sign-in ' for automatic creation of OTP tokens.

To enable MFA for Web admin console access, Enable Require MFA for 'Web admin console'

To enable MFA for remote access VPN (IPsec and SSL VPN), Enable Require MFA for 'SSL VPN remote access' and 'IPSec remote access'

## Remediation:

Navigate to ' Configure ' > 'Authentication' > 'Multi-factor authentication' > 'Multi-factor authentication settings'

Select ' Specific Users and groups ' > ' Add the user or group '

Enable ' Generate OTP toles with next sign-in ' for automatic creation of OTP tokens.

To enable MFA for Web admin console access, Enable Require MFA for 'Web admin console'

To enable MFA for remote access VPN (IPsec and SSL VPN), Enable Require MFA for 'SSL VPN remote access' and 'IPSec remote access'

## Default Value:

By default MFA configuration for Web admin console and remote access VPN (IPSec and SSL VPN) is not enabled

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/OneTimePassword/index.html>

## 1.1.9 Ensure MFA for default admin (Manual)

### Profile Applicability:

- Level 1

### Description:

Implementing MFA strengthens the security of firewall console access by requiring an additional verification step, helping ensure that only authorized administrators can make changes to firewall configurations.

### Rationale:

Firewall web console provides high-privileged access, so enforcing MFA reduces the risk of unauthorized configuration changes and any harmful changes to the critical network security policies

### Audit:

Navigate to ' System ' > 'Administration' > 'Device Access ' > 'Multi-factor Authentication for default admin'

Turn ' ON ' MFA for default admin

MFA doesn't apply to SSH sign-ins, allowing you to recover the account

### Remediation:

Navigate to ' System ' > 'Administration' > 'Device Access ' > 'Multi-factor Authentication for default admin'

Turn ' ON ' MFA for default admin

MFA doesn't apply to SSH sign-ins, allowing you to recover the account

### Default Value:

By default, MFA for default admin is disabled

### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/DeviceAccess/index.html>

## 1.1.10 Set Hostname (Automated)

### Profile Applicability:

- Level 1

### Description:

A hostname on a Sophos Firewall is simply the human-friendly name assigned to the device. It identifies the firewall on the network, in logs, in monitoring systems, and in Sophos Central.

### Rationale:

A meaningful hostname ensures that:

- Syslog, SNMP traps, email alerts, and SIEM logs clearly identify which firewall the event came from.
- Troubleshooting in multi-firewall environments becomes much easier.

Without a hostname, logs may default to an IP or generic device name, which creates confusion—especially in SOC or audit workflows.

### Audit:

#### GUI

Log in to the Sophos Firewall Web Admin.  
Look at the top-left corner of the dashboard – the hostname is displayed there.  
Or navigate to:  
Administration → Device Access → Hostname  
(In older versions: System → Administration → Hostname)

#### CLI

SSH into the firewall or open the console.  
Log in.  
Enter the Advanced Shell:  
  
Run:  
hostname  
or:  
get hostname  
  
Both commands will display the current hostname.

### Remediation:

#### GUI

Log in to the Sophos Firewall Web Admin portal.  
In the left navigation menu, go to:  
Administration → Device Access → Hostname  
(In older SFOS versions, it appears under: System → Administration → Hostname ).  
You will see fields for:

Hostname  
Domain name  
Device description (optional)

Enter the new Hostname (e.g., FW-HQ-EDGE01).  
Click Apply or Save at the top or bottom of the page.  
The system may prompt you to re-login for the change to appear everywhere.

## CLI

Connect to the firewall via SSH or the serial console.  
Log in with your admin credentials.  
Enter the advanced shell:

(or directly type)  
set hostname <your-hostname>

Example:  
set hostname SFOS-DEN-EDGE01

Press Enter, then exit the shell.



## 1.2 SNMP & Device Notification Settings

Device Notification Settings section contains setting up SNMP server and email settings on how the device sends notification for critical events that need administrator's attention.

## 1.2.1 Ensure SNMPv3 is selected for queries and traps (Automated)

### Profile Applicability:

- Level 1

### Description:

SNMP (Simple Network Management Protocol) gives access to Sophos Firewall information such as status of the firewall, service availability, CPU, memory and disk usage. Although Sophos Firewall supports SNMPv1 and SNMPv2c protocols, you should always use SNMPv3 for user and the authorized hosts to send traps. Specify encryption and authentication settings to ensure confidentiality, message integrity, and user validity.

### Rationale:

SNMPv3 utilizes AES-128 encryption, message integrity, user authorization, and device authentication security features. SNMPv2c does not provide these security features. If an SNMPv2c community string is intercepted or otherwise obtained, an attacker could gain read access to the firewall. Note that SNMP write access is not possible.

### Audit:

Navigate to `System > Administration > SNMP`.

Verify that SNMPv1 and v2 are not configured.

Verify that `SNMPv3 users and traps > Encryption algorithm` is configured with either AES or DES. Set appropriate password strength for both authentication and encryption.

### Remediation:

Navigate to `System > Administration > SNMP`.

Remove insecure SNMPv1 and v2 configurations.

Set `SNMPv3 users and traps > Encryption algorithm` is configured with either AES or DES. Set appropriate password strength for both authentication and encryption.

### Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/SNMP/AdministrationSNMPAgentConfigure/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/SNMP/AdministrationSNMPUserAdd/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                                                                              |                                                                                       |    |    |
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.                                 |    |    |    |
| v8               | <b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b><br>Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |  |  |
| v8               | <b>6.5 <u>Require MFA for Administrative Access</u></b><br>Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.                                                         |  |  |  |
| v7               | <b>4.5 <u>Use Multifactor Authentication For All Administrative Access</u></b><br>Use multi-factor authentication and encrypted channels for all administrative account access.                                                                                              |                                                                                       |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                                 |                                                                                       |  |  |
| v7               | <b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b><br>Encrypt all sensitive information in transit.                                                                                                                                                             |                                                                                       |  |  |

## *1.2.2 Ensure notification is configured to send system and security events (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

This recommendation ensures that administrator receives notification on system events, reports and security incidents either via email or SNMP Traps.

### **Rationale:**

Verify the notification settings to ensure that correct email address of sender "From Email Address" and recipient "Send notification to email address" is configured. Both settings should be reflected according to the rightful sender and recipient together with notification list for admin, system, security events.

### **Impact:**

This recommendation ensures that administrator receives the notifications for critical system, security events and reports.

## Audit:

Navigate to `System > Administration > Notification settings > Mail server settings`.

Verify that `Send notification via > Built-in email server` or `External email server` is checked and configure email settings appropriately.

Navigate to `Configure > System services > Notification list`.

Verify that appropriate admin, system and security events are checked to send email notification and/or SNMP traps.

## Remediation:

Navigate to `System > Administration > Notification settings`.

When `built-in email server` is used.

Set the `from email address` of the sender.

Set the `Send notifications to email address` of the administrators' email address.

Set `Management interface IP address` to send notification from.

When `External mail server` is used.

Set the `Mail server IPv4 address/FQDN - Port` is set to the outgoing mail server.

Set `username` and `password` to authenticate to the outgoing mail server. Set `connection security` to `STARTTLS` or `SSL/TLS`.

Navigate to `Configure > System services > Notification list`.

Set the appropriate admin, system and security events to send email notification and/or SNMP traps.

## Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/EmailNotificationSettings/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                              | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>13.1 <u>Centralize Security Event Alerting</u></b><br>Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard. |      |  |  |
| v8               | <b>13.11 <u>Tune Security Event Alerting Thresholds</u></b><br>Tune security event alerting thresholds monthly, or more frequently.                                                                                                                                                                                                                                                  |      |                                                                                     |  |
| v7               | <b>0.0 <u>Explicitly Not Mapped</u></b><br>Explicitly Not Mapped                                                                                                                                                                                                                                                                                                                     |      |                                                                                     |                                                                                     |

## **2 User Identification & Authentication**

All the users accessing the network resources should be authenticated by Firewall. Once authentication is successful, Sophos Firewall communicates with directory servers to get additional authorization data for access control.

While the users are on the network, Sophos Firewall can identify and map according to the username instead of IP addresses and establish Identification, Authentication, Authorization and Accountability(IAAA).

## *2.1 Ensure Firewall rules are configured to identify users before authorizing access (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Configure appropriate settings to map IP addresses to usernames. Mapping users to IP addresses is what permits the firewall to create rules based on users and groups rather than IP addresses and subnets, as well as log events by usernames rather than IP addresses or DNS names. The specifics of how to achieve IP-to-username mapping is highly dependent on the environment. It can be enabled by integrating the firewall with a domain controller, captive portal, Terminal Server, Kerberos, NTLM, and synchronized security heartbeat from a variety of devices.

### **Rationale:**

Understanding which user is involved in a security incident allows appropriate personnel to move quickly between the detection and reaction phases of incident response. In environments with either short DHCP lease times, or where users may move frequently between systems, the ability to analyze or report, or alert on events based on user accounts or user groups is a tremendous advantage. For forensics tasks when DHCP lease information may not be available, the Source User information may be the only way to tie together related data.



## Audit:

Validate allowed firewall rules with source zone (LAN/DMZ) are configured with user identification. Source network where users are located must authenticate to Sophos Firewall first before accessing network resources.

Verify that `Protect > Rules and policies > Firewall rules` and within the firewall rule ensure `Match known users` is checked and add authorized `User or groups`. Captive portal redirects to unknown users by ensuring `Use web authentication for unknown users` is checked.

## Remediation:

To enable user based firewall rule:

Navigate to `Protect > Rules and policies > Firewall rules` edit existing policies or when creating a new firewall policy `match known users` is checked.

`Log firewall traffic` is checked to log for allowed traffic.

Configure authentication server to use for firewall connections.

Navigate to `Configure > Authentication > Services > Firewall authentication methods` move the primary authentication server at the top.

Configure Clientless users for devices such as printers and IoT devices that unable to authenticate with standard authentication options.

To add the devices to clientless users, navigate to `Configure > Authentication > Clientless users > Add or Add range`

In Active directory environment AD SSO can be configured to allow unauthenticated web access. Sophos Firewall also supports Authentication using Microsoft Entra ID SSO

Navigate to `Configure > Authentication > Web Authentication > Authorize unauthenticated users for web access > Kerberos & NTLM` and `show captive portal link` is checked.

In Window only environment clientless SSO can be configured to authenticate with Sophos Firewall based on security logon events at the Domain Controllers.

Navigate to `Configure > Authentication > STAS > Enable Sophos Transparent Authentication Suite > Add new collector` and `Restrict client traffic during identity probe > Yes`.

Refer to the reference section for more information with the configuration.

## Default Value:

Not configured.

## References:

1. "How to configure Authentication Server" - <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/AuthenticationServices/index.html>
2. "Clientless SSO in a single AD Domain Controller Environment?" - <https://community.sophos.com/kb/en-us/123156>
3. "How to configure clientless users" – <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/ClientlessUsers/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                 | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets. |    |    |    |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                  |  |  |  |
| v7               | <b>16.13 Alert on Account Login Behavior Deviation</b><br>Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.  |                                                                                       |                                                                                       |  |

## *2.2 Ensure Encrypted connection is used in connecting external Active Directory and LDAP (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Microsoft has made secure connections mandatory for recent server versions. The security of the communication can be significantly improved for LDAP simple binds that are performed over SSL/TLS connections.

### **Rationale:**

Unsigned network traffic is susceptible to replay attacks in which an intruder intercepts the authentication attempt and the issuance of a ticket. The intruder can reuse the ticket to impersonate the legitimate user. Additionally, unsigned network traffic is susceptible to man-in-the-middle (MiTM) attacks in which an intruder captures packets between the client and the server, changes the packets, and then forward them to the server.

### **Audit:**

Navigate to `Configure > Authentication > Servers > Edit` and verify that `Connection security` is selected with either `SSL/TLS` or `STARTTLS` is used and `Validate server certificate` is checked.

### **Remediation:**

Navigate to `Configure > Authentication > Servers > Edit or Add` and set `Connection security` with either `SSL/TLS` or `STARTTLS` and `Validate server certificate` is checked.

### **Default Value:**

Not configured.

### **References:**

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/Servers/AuthenticationServerAdd/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>12.3 <u>Securely Manage Network Infrastructure</u></b><br>Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS. |      |  |  |
| v7               | <b>11.5 <u>Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions</u></b><br>Manage all network devices using multi-factor authentication and encrypted sessions.                                                      |      |  |  |

### **3 System Services, Firmware and Updates**

This section covers High Availability (HA) and Sophos firewall update of Sophos X-Ops, AV, IPS, Application signatures, WAF, firmware and security related hotfixes.

### *3.1 Ensure "Fully Synchronized" High Availability peer is configured (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

High Availability (HA) is a clustering technology that is used to maintain uninterrupted service in the event of power, hardware, or software failure. Sophos Firewall devices can be configured in Active-Active or Active-Passive HA modes. The Devices (The Primary and Auxiliary Device) are physically connected over a dedicated HA link port.

#### **Rationale:**

To ensure availability of both the firewall and the resources it protects, a High Availability peer is required. In the event a single firewall fails, or when maintenance such as a firmware update is required, the HA peer can be used to automatically fail over session states and maintain overall availability of the network.

#### **Impact:**

Not configuring High Availability (HA) correctly directly impacts the availability of the system. With HA in place, standard maintenance such as OS updates, network and power cabling changes can be accomplished with no outage or a minimum impact.

## Audit:

Navigate to `Configure > System Services > High Availability > High Availability Status`.  
Verify that `HA status` is either `Established[Active-Passive]` or `Established[Active-Active]` and confirm `Local` and `Peer` devices are not showing `Standalone` or `Faulty`.

Navigate to `High Availability Configuration > Select ports to be monitored`.  
Verify that correct interfaces are monitored.

`Keepalive request interval` and `Keepalive attempts` should be set to optimal setting or remain default value of `250` milliseconds and `16` attempts respectively.

## Remediation:

HA can be configured in two modes: QuickHA mode and Interactive mode.

In QuickHA mode, Initial device role, Node name and Dedicated HA link is specified on each device.

In Interactive mode, all the settings are specified such as monitored port, keep alive values and the preferred primary device.

Navigate to `Configure > System Services > High Availability > High Availability Status`.  
When `Local` and `Peer` devices are shown as `Standalone` or `Faulty`, connection to the auxiliary device could be lost or becomes a faulty node, re-configure HA and sync auxiliary device to a working state.

Navigate to `High Availability Configuration > Select ports to be monitored`.  
Set the correct interfaces to be monitored.

Configure default value of `Keepalive request interval` to `250` milliseconds and `Keepalive attempts` to `16` attempts or set to optimal setting respectively.

## Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/HighAvailabilityStartupGuide/HAConfiguration/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/HighAvailabilityStartupGuide/HAConfiguration/HASharedConfigureActivePassive/index.html>

3. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/HighAvailabilityStartupGuide/HAConfiguration/HAQuickHAConfigureActiveActive/index.html>

#### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |



### *3.2 Ensure 'Pattern updates' is set to download and install updates every 15 minutes (Automated)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

Set Pattern download/installation to 'auto update' and interval of 'every 15 minutes'

#### **Rationale:**

New protection patterns may be released at any time. With frequent update schedule, the firewall can ensure threats with new definitions are quickly mitigated. A daily update schedule could leave an organization vulnerable to a known virus for nearly 24 hours, in a worst-case scenario. Setting an appropriate threshold value reduces the risk of a bad definition file negatively affecting traffic.

#### **Impact:**

Sophos X-Ops patterns, AV signatures, GeoIP database, IPS and application signatures to block immediate, active threats to the environment. With a 15 minutes update schedule, the firewall can ensure threats with new definitions are quickly mitigated.

## Audit:

Navigate to `System > Backup & Firmware > Pattern Updates`.

Verify that `Pattern download/installation > Auto update` is set to `ON`.

Verify that `Interval` is set to `Every 15 minutes`.

Verify that `Pattern` `Last successful update` is showing `Success`

For an Air-gap environment patterns can also be downloaded manually. The pattern file can be downloaded from the below link

<https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/PatternManage/index.html#manual-pattern-update>

Navigate to 'System > Backup & Firmware > Manual pattern updates > Upload the pattern file'

## Remediation:

Navigate to `System > Backup & Firmware > Pattern Updates`.

Set `Pattern download/installation > Auto update` to `ON`.

Set the download `Interval` to `Every 15 minutes`.

When the `Pattern` `Last successful update` is not showing `Success`, click `Update pattern now` to download the updates manually.

## Default Value:

Enabled Default Value is 2 hours

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/PatternManage/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                  | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>7.3 <u>Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis. |  |  |  |

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>7.4 <u>Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |  |  |  |
| v7               | <b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b>3.5 <u>Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

### 3.3 Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes' (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Set hotfixes to be applied automatically whenever there is an out-of-band security update is available for the device.

#### Rationale:

Security updates of the firewall can be released at any time. To ensure the firewall and the rest of the network remain protected from known vulnerability hotfixes should be allowed and device can be applied automatically. Status of Hotfix is checked from Sophos CLI.

#### Audit:

```
Access Sophos CLI `Select Option 4> system hotfix show`.
```

```
Verify that `system hotfix show output is Hotfix is enabled`.
```

#### Remediation:

```
Access Sophos CLI `Select Option 4> system hotfix show`.
```

```
Verify that `system hotfix show output is Hotfix is enabled`.
```

#### Default Value:

This setting is enabled by default.

#### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/CommandLineHelp/DeviceConsole/SystemCommands/Hotfix/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b><u>7.3 Perform Automated Operating System Patch Management</u></b><br>Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                              |  |  |  |
| v8               | <b><u>7.4 Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                        |  |  |  |
| v7               | <b><u>3.4 Deploy Automated Operating System Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.      |  |  |  |
| v7               | <b><u>3.5 Deploy Automated Software Patch Management Tools</u></b><br>Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor. |  |  |  |

### *3.4 Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency (Manual)*

#### **Profile Applicability:**

- Level 1

#### **Description:**

Set Sophos Firewall to send encrypted backup of the configuration to administrators' email address or store at the backup FTP server.

#### **Rationale:**

Hardware or software failure can happen any time. In the event network needs to be restored immediately, ensure the backup snapshot of the configuration is taken at regular interval and store in secure encrypted format at the redundant location to restore at the new device.

## Audit:

Navigate to `System > Backup & Firmware > Backup & Restore > Backup`. Backup mode is set to either `FTP` or `Email`.

When `Backup mode` is set to `FTP`, verify that `FTP server IP`, `Username` or `FTP password` is set.

When `Backup mode` is set to `Email` verify that `Email Address` is set to the administrators' email address.

Verify that `Frequency` is set to `Daily, Weekly or Monthly`.

Verify that `Encryption password` is set and ensure that encrypted backup can be sent successfully.

## Remediation:

Navigate to `System > Backup & Firmware > Backup & Restore > Backup`. Backup mode is set to either `FTP` or `Email`.

When `Backup mode` is set to `FTP`, configure `FTPserver IP`, `Username` or `FTP password`.

When `Backup mode` is set to `Email`, configure `Email Address` to the administrators' email address.

`Frequency` is set to `Daily, Weekly or Monthly`.

Set strong `Encryption password` and ensure that encrypted backup can be sent successfully. Store the `Encryption password` in secure location for future recovery.

## Default Value:

Not enabled.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                         | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.2 Perform Automated Backups</b><br>Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data. |  |  |  |

| Controls Version | Control                                                                                                                                                                                                                                                                            | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>11.3 <u>Protect Recovery Data</u></b><br>Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements.                                                                                                   |    |    |    |
| v8               | <b>11.4 <u>Establish and Maintain an Isolated Instance of Recovery Data</u></b><br>Establish and maintain an isolated instance of recovery data. Example implementations include, version controlling backup destinations through offline, cloud, or off-site systems or services. |    |    |    |
| v7               | <b>10.1 <u>Ensure Regular Automated Back Ups</u></b><br>Ensure that all system data is automatically backed up on regular basis.                                                                                                                                                   |    |    |    |
| v7               | <b>10.2 <u>Perform Complete System Backups</u></b><br>Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.                                                  |    |    |    |
| v7               | <b>10.4 <u>Ensure Protection of Backups</u></b><br>Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.                        |    |    |    |
| v7               | <b>10.5 <u>Ensure Backups Have At least One Non-Continuously Addressable Destination</u></b><br>Ensure that all backups have at least one backup destination that is not continuously addressable through operating system calls.                                                  |  |  |  |



## 3.5 Ensure No Expired Subscription Licenses (Manual)

### Profile Applicability:

- Level 1

### Description:

Licensing is used to enable various features on Sophos Firewall regardless whether the license is for hardware or software/virtual firewall.

### Rationale:

Active subscription will ensure the device is getting up-to-date signatures for both known and unknown threats and remain functional for services requires cloud lookup.

### Impact:

Expired subscription will lapse security updates which will impact the security effectiveness of the feature/functionality.

### Audit:

Navigate to `System > Administration > Licensing`.

Verify under `Module subscription details` under `Status` to ensure there is no expired licenses for all the subscriptions.

### Remediation:

Navigate to `System > Administration > Licensing`.

Under `Module subscription details` and click `Synchronize` to connect to the licensing server to get latest subscription details. Or contact Sophos immediately to renew the expired licenses.

### References:

1. <https://docs.sophos.com/central/customer/help/en-us/LicensingGuide/FirewallLicenses/SFOSLicensingModel/index.html>
2. <https://docs.sophos.com/central/customer/help/en-us/LicensingGuide/FirewallLicenses/index.html>
3. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                     | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>7.4 <u>Perform Automated Application Patch Management</u></b><br>Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.                                                                                                                                                              |    |    |    |
| v8               | <b>10.2 <u>Configure Automatic Anti-Malware Signature Updates</u></b><br>Configure automatic updates for anti-malware signature files on all enterprise assets.                                                                                                                                                                                             |    |    |    |
| v8               | <b>12.1 <u>Ensure Network Infrastructure is Up-to-Date</u></b><br>Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support. |    |    |    |
| v7               | <b>8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u></b><br>Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.                                                                                                                                                    |    |    |    |
| v7               | <b>11.4 <u>Install the Latest Stable Version of Any Security-related Updates on All Network Devices</u></b><br>Install the latest stable version of any security-related updates on all network devices.                                                                                                                                                    |  |  |  |

### 3.6 Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode" (Manual)

#### Profile Applicability:

- Level 2

#### Description:

IKEv1 Aggressive Mode does not provide Peer Identity Protection. They are vulnerable to offline dictionary or brute force attack.

#### Rationale:

As stated in CVE-2002-1623, the design of the Internet Key Exchange (IKE) protocol, when using Aggressive Mode for shared secret authentication, does not encrypt initiator or responder identities during negotiation, which may allow remote attackers to determine valid usernames by monitoring responses before the password is supplied or sniffing.

#### Impact:

The use of IKEv1 with Aggressive Mode has considerable confidentiality impact.

#### Audit:

```
Navigate to `System > Profiles > IPsec profiles`.
Verify that active `IPsec Profile` in used is not configured with `Key
exchange` `IKEv1` and `Authentication mode` `Aggressive mode`.
```

#### Remediation:

```
Navigate to `System > Profiles > IPsec profiles`.
Remove any active `IPsec Profiles` configured with `Key exchange` `IKEv1` and
`Authentication mode` `Aggressive mode` and replace with `IKEv2` or `Main
mode`.
```

#### Default Value:

Not configured.

#### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Profiles/IPsecProfiles/index.html>

**CIS Controls:**

| Controls Version | Control                                                                                                                                                                                                         | IG 1 | IG 2                                                                                | IG 3                                                                                |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                 |      |  |  |
| v7               | <b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b><br>Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. |      |  |  |

### *3.7 Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Sophos Firewall provides extensive logging capabilities for traffic, system, and network protection functions. You can use logs to analyze network activity to help identify security issues and reduce network abuse.

You can store logs locally, send them to Sophos Central, or send them to third-party syslog servers.

You can select logs to store or send by module or feature, or you can select all logs.

#### **Rationale:**

##### **Firewall**

Firewall logs provide information about traffic associated with the firewall configuration, such as firewall rules, MAC filtering, and DoS attacks.

##### **Web-content policy**

Web content policy logs shows the details about the websites accessed by the user that contain the terms mentioned in the content filter and the taken action

##### **IPS**

IPS logs provide records of detected and dropped attacks based on suspicious patterns (anomalies) and signatures.

##### **Malware**

Malware logs provide details of viruses detected in HTTP, SMTP, FTP, POP3, IMAP4, HTTPS, SMTPS, IMAPS, and POPS traffic.

##### **Email**

Email logs provide details about SMTP, POP3, IMAP4, SMTPS, POPS, IMAPS spam, and probable spam mails.

##### **Web filter**

Web filter logs provide details about web and filtering events associated with web policies.

##### **Application filter**

Application filter logs provide details about denied Applications associated with Application policies

### **SSL/TLS Inspection**

SSL/TLS Inspection logs provide details about the SSL traffic details such as action taken, decryption profile etc.

### **VPN**

VPN logs details about the VPN connectivity status, any error messages

### **Admin**

Event logs provide information about configuration activities and system activities.

### **Authentication**

Authentication logs provide information about authentication activities

### **SD-WAN**

SD-WAN logs provide details such as SD-WAN profile used, Gateway associated with the traffic

### **Web server protection**

Web server protection logs provide details of web server protection activities, for example, protection policies.

### **Advanced threat response**

Advanced threat response logs provide information about ATR events such as drops or alerts.

### **Wireless**

Wireless logs provide details about access point activity and SSIDs.

### **Security Heartbeat**

Heartbeat logs provide information about the health status of the endpoints.

### **System**

System health logs provide details of CPU usage, memory usage, number of live users, interfaces, and disk partitions.

### **Zero-day protection**

Zero-day protection logs provide records of all Zero-day protection events.

## Audit:

Navigate to `Protect > Rules and policies`.  
Verify the configured Firewall rules and ensure `Log firewall traffic` is checked.

Navigate to `Configure > System services > Log settings`.  
Verify that external syslog server is configured and sending system, security events to external syslog server.

Navigate to 'Monitor & Analyze > Diagnostics > Tools > Troubleshooting logs and Consolidated troubleshooting report'  
You can download individual log files or download a consolidated log file.

Sophos Firewall helps you record the changes administrators make on the web admin console or CLI, via the configuration-audit.logs

Navigate to 'Monitor & Analyze > Diagnostics > Tools > Troubleshooting logs > configuration-audit.log'

## Remediation:

Navigate to `Protect > Rules and policies`.  
Set `Log firewall traffic` is checked for configured firewall rules.

Navigate to `Configure > System services > Log settings`.  
Configure external syslog server and set to send system, security events to external syslog server.

Navigate to 'Monitor & Analyze > Diagnostics > Tools > Troubleshooting logs and Consolidated troubleshooting report'  
You can download individual log files or download a consolidated log file.

Sophos Firewall helps you record the changes administrators make on the web admin console or CLI, via the configuration-audit.logs

Navigate to 'Monitor & Analyze > Diagnostics > Tools > Troubleshooting logs > configuration-audit.log'

## Default Value:

Not configured. configuration audit is enabled by default

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SystemServices/LogSettings/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                        |  |    |    |
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |    |    |
| v8               | <b>8.11 <u>Conduct Audit Log Reviews</u></b><br>Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis.                                                                                    |                                                                                     |    |    |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |    |    |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                     |   |   |
| v7               | <b>6.7 <u>Regularly Review Logs</u></b><br>On a regular basis, review logs to identify anomalies or abnormal events.                                                                                                                                                                                  |                                                                                     |  |  |
| v6               | <b>6.4 <u>Regularly Monitor Logs For Anomalies</u></b><br>Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.                                                      |                                                                                     |                                                                                       |                                                                                       |



## 4 Advanced Threat & Synchronized Security

Active Threat response provides an instant and automated response to active adversaries. Active threat response offers multiple modules of threat intelligence feeds, enabling the firewall to coordinate defenses immediately without manual intervention. The modules are as follows.

1. MDR threat feeds
2. NDR Essentials
3. Sophos X-Ops threat feeds
4. Third-party threat feeds.

One can choose to configure some or all of them. Threat feeds are a list of IP address, domains and URLs involved in threat activity, such as phishing and malware. Depending on the thread feed module, the firewall remain up-to-date with the threat feeds latest indicators at frequent intervals or based on threat information

#### *4.1 Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop' (Manual)*

##### **Profile Applicability:**

- Level 2

##### **Description:**

Sophos X-Ops threat feeds is a SophosLabs managed global threat database that is regularly updates and pushed to the firewall. The firewall blocks all requests and traffic matching this database of malicious IP addresses, domains and URLs.

##### **Rationale:**

Using Sophos X-Ops threat feeds, you can quickly detect compromised clients in your network and raise an alert or drop the traffic from those clients.

## Audit:

Navigate to `Protect > Advanced threat response > Sophos X-Ops threat feeds (Advanced threat protection) > Sophos X-Ops threat feeds`.

Verify that `Sophos X-Ops threat feeds` is 'Enabled'

Verify that action is set to `Log and drop`.

Verify that wide range of network/host IP addresses are not added to `Host and network Exceptions`.

Verify that wide range of domains, URLs or IP addresses are not added to `Threat Exceptions` that may expose network to the security risks.

## Remediation:

Navigate to `Advanced threat response > Sophos X-Ops threat feeds (Advanced threat protection) > Sophos X-Ops threat feeds`.

Enable Sophos X-Ops threat feeds

Set the action to `Log and drop`.

Remove unnecessary exemption from network and threat exceptions.

## Default Value:

Not enabled.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ConfigureFeeds/ActiveThreatResponseSophosXOpsThreatFeeds/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/Requirements/licenses/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                        |  |  |  |
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                     |  |  |

## *4.2 Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

By enabling 'Use Zero-day protection' at the firewall rule increases the possibility of identifying unknown viruses. And ensure administrator does not exclude file types from Zero-day protection analysis.

### **Rationale:**

When a user downloads a file from the internet via HTTP/S, FTP protocol and the file contains active content or unknown reputation that cannot be easily detected by signature-based AV engine, it will be uploaded to SOPHOS cloud sandboxing service for additional analysis. Accidental exclusion of file type at Zero-day protection settings configuration will reduce the security effectiveness.

### **Impact:**

With Zero-day protection is unchecked, users may unknowingly download files that have not been seen by AV engines or weaponized office documents. Exclude file types in the Zero-day protection settings could also bypass broad range of true filetype from uploading to the cloud for additional analysis.

## Audit:

For firewall rules that allowed outbound traffic to the internet should be enabled with 'Use zero-day protection'.

Navigate to 'Protect > Rules and policies > Firewall rules' existing firewall rule with allowed outbound traffic and verify 'Security features > Web filtering > Malware and content scanning > Scan HTTP and decrypted HTTPS', 'Use zero-day protection' and 'Scan FTP for malware' is checked.

Navigate to 'Monitor & Analyze > Zero-day protection > Protection Settings' and verify 'Exclude file types' to ensure there are no file type is exempted from Sandbox analysis.

## Remediation:

Navigate to 'Protect > Rules and policies > Firewall rules' existing firewall rule with allowed outbound traffic and configure 'Security features > Web filtering > Malware and content scanning > Scan HTTP and decrypted HTTPS', 'Use Zero-day protection' and 'Scan FTP for malware' is checked.

Navigate to 'Monitor & Analyze > Zero-day protection > Protection Settings' and remove file type exceptions from 'Exclude file types'.

## Default Value:

Not enabled

## References:

1. [https://support.sophos.com/support/s/article/KB-000036080?language=en\\_US](https://support.sophos.com/support/s/article/KB-000036080?language=en_US)
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ZeroDayProtection/ZeroDayProtectionSettings/index.html>
3. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ZeroDayProtection/ZeroDayDownloadsAndAttachments/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                      | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>10.1 Deploy and Maintain Anti-Malware Software</b><br>Deploy and maintain anti-malware software on all enterprise assets. |  |  |  |

| Controls Version | Control                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>10.2 <u>Configure Automatic Anti-Malware Signature Updates</u></b><br>Configure automatic updates for anti-malware signature files on all enterprise assets.                                              |  |  |  |
| v8               | <b>10.6 <u>Centrally Manage Anti-Malware Software</u></b><br>Centrally manage anti-malware software.                                                                                                         |                                                                                     |  |  |
| v7               | <b>8.1 <u>Utilize Centrally Managed Anti-malware Software</u></b><br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. |                                                                                     |  |  |
| v7               | <b>8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u></b><br>Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.     |  |  |  |

### *4.3 Ensure Zero-day protection is enabled for Email Protection and set to MTA mode (Manual)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

By enabling 'Use zero-day protection' at the SMTP policy increases the possibility of identifying unknown viruses delivered through email gateway.

#### **Rationale:**

Targeted attacks with Email attachments that contain zero-day viruses and weaponized office documents could be thwarted at the Email gateway by scanning at the SMTP proxy before routed to the internal email server. Accidental exclusion of file type at Sandbox configuration will reduce the security effectiveness.

#### **Impact:**

Zero-day viruses and Advanced Persistent Threats (APT) can be delivered via weaponized office documents as a form of attachment to the business email. By setting appropriate malware protection setting to scan for viruses and detect zero-day threats with Zero-day protection before delivering the emails to the MTA.



## Audit:

This configuration option is only applicable when the device is configured with `MTA mode` and set `Sophos` as primary malware scanning engine.

Navigate to `Protect > Email`. Verify the existing SMTP policy `Malware protection > Scanning > Single anti-virus (this set the scan engine to Sophos )` is set and Selected antivirus action` to `Drop`. Email attachment successfully verified by antivirus engine as malicious should be set to `Drop`.

`Quarantine unscannable content` is checked to prevent files with multiple layers of compression and password protected archives files that cannot be scanned by antivirus engine should be `quarantined`.

Verify that `Use zero-day protection` should be checked

## Remediation:

This configuration option is only applicable when the device is configured with `MTA mode` and set `Sophos` as primary malware scanning engine.

Navigate to `Protect > Email`. Verify the existing SMTP policy and set `Malware protection > Scanning > Single anti-virus( this set the scan engine to Sophos)` is set and Selected antivirus action` to `Drop`. Email attachment successfully verified by antivirus engine as malicious should be set to `Drop`.

`Quarantine unscannable content` is checked to prevent files with multiple layers of compression and password protected archives files that cannot be scanned by antivirus engine should be `quarantined`.

Set `Use zero-day protection` is checked

## Default Value:

Not configured.

## References:

1. [https://support.sophos.com/support/s/article/KB-000036080?language=en\\_US](https://support.sophos.com/support/s/article/KB-000036080?language=en_US)
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Email/PoliciesExceptions/EmailSMTPRouteAndScanPolicyAdd/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                      | IG 1 | IG 2 | IG 3 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>9.7 <u>Deploy and Maintain Email Server Anti-Malware Protections</u></b><br>Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.                     |      |      | ●    |
| v8               | <b>10.1 <u>Deploy and Maintain Anti-Malware Software</u></b><br>Deploy and maintain anti-malware software on all enterprise assets.                                                                          | ●    | ●    | ●    |
| v8               | <b>10.2 <u>Configure Automatic Anti-Malware Signature Updates</u></b><br>Configure automatic updates for anti-malware signature files on all enterprise assets.                                              | ●    | ●    | ●    |
| v8               | <b>10.6 <u>Centrally Manage Anti-Malware Software</u></b><br>Centrally manage anti-malware software.                                                                                                         |      | ●    | ●    |
| v7               | <b>8.1 <u>Utilize Centrally Managed Anti-malware Software</u></b><br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers. |      | ●    | ●    |
| v7               | <b>8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u></b><br>Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.     | ●    | ●    | ●    |

## *4.4 Ensure Synchronized Security Heartbeat is enforced on Firewall Rules (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Security Heartbeat enables Sophos Firewall and endpoints managed by Sophos Endpoint Protection to communicate through Sophos Central and exchange information on the endpoints' security status, the so-called health status. Sophos Firewall administrators as well as Sophos Central administrators are able to define policies for network access based on the endpoints' health status. Endpoints with security incidents can be immediately isolated thus preventing threats to spread across the network.

### **Rationale:**

Sophos Endpoint Protection ensures that the endpoint belongs to the organization and has permission to access the network. These endpoints send at regular intervals updates about their health status to Sophos Firewall which in turn applies the defined policies based on that information.

### **Impact:**

Missing heartbeat or endpoint with compromised state should not be allowed to connect to servers, internet and other devices within the network. Synchronized security heartbeat can identify the source of infection and isolate the device from the rest of the network.

## Audit:

Navigate to `System > Sophos Central`.  
Verify that `Security Heartbeat` is turned `ON`.

Check that Sophos firewall is registered to Sophos Central, configured to receive Heartbeat from the Sophos Endpoints.

Navigate to `Protect > Rules and Policies > Firewall rules`.  
Filter `Rule type >` `Network` and `User`, filter `source zone > LAN` and `DMZ`.  
Verify on the configured firewall rule `Configure Synchronized Security Heartbeat` and check that `Minimum source HB permitted` is set to `Green` or `Yellow`.

If the rule is configured to allow Egress traffic with clients are connecting resources on `WAN` zone, `Minimum source HB permitted` should be configured with either `Green` or `Yellow` for tighter security control.

If the rule is configured to allow traffic between `LAN` to `DMZ` zones with communication between Sophos protected Endpoints and Server, please consider additional control with setting both `Minimum source HB permitted` and `Minimum destination HB permitted` to either `Green` or `Yellow`.

## Remediation:

Navigate to `System > Sophos Central > Register` .

Register Sophos Firewall to Sophos Central, set `Security Heartbeat` to `ON`.

Navigate to `Protect > Rules and Policies`.  
Filter `Rule type > Network` and `User`, filter `source zone > LAN` and `DMZ`.  
Navigate to configured firewall rule with `Configure Synchronized Security Heartbeat`.

Set `Minimum source HB permitted` to `Green` or `Yellow`.

If the rule is configured to allow Egress traffic with Sophos Endpoints are connecting resources on `WAN` zone, set `Minimum source HB permitted` to either `Green` or `Yellow` for tighter security control.

If the rule is configured to allow traffic between `LAN` to `DMZ` zones with communication between Sophos protected Endpoints and Server, configure additional control with setting both `Minimum source HB permitted` and `Minimum destination HB permitted` to either `Green` or `Yellow`.

## Default Value:

Not configured.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/SophosCentral/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                             | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                                                                                                                      |  |    |    |
| v8               | <b>10.6 <u>Centrally Manage Anti-Malware Software</u></b><br>Centrally manage anti-malware software.                                                                                                                                                                                                                                                                                                |                                                                                     |    |    |
| v8               | <b>12.8 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u></b><br>Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access. |                                                                                     |                                                                                       |    |
| v7               | <b>8.1 <u>Utilize Centrally Managed Anti-malware Software</u></b><br>Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.                                                                                                                                                                                        |                                                                                     |  |  |
| v7               | <b>8.6 <u>Centralize Anti-malware Logging</u></b><br>Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.                                                                                                                                                                                                             |                                                                                     |  |  |
| v7               | <b>11.7 <u>Manage Network Infrastructure Through a Dedicated Network</u></b><br>Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.                                                           |                                                                                     |  |  |

## 4.5 Ensure MDR Threat Feeds is enabled (Manual)

### Profile Applicability:

- Level 2

### Description:

MDR Threat Feeds is Sophos Managed Detection and Response (MDR) service that is integrated with the firewall. Sophos MDR analysts can push threat intelligence to the firewall directly from Sophos Central, allowing the firewall to coordinate defenses immediately. The feed is based on your network's traffic related to malicious servers. The firewall automatically blocks traffic based on the IPv4 addresses, domains, and URLs in the MDR threat feeds.

### Rationale:

MDR Analyst can push threat intelligence to the firewall directly from Sophos Central in real time which allows the firewall to coordinate defenses. The traffic is blocked based on IPv4 addresses, domains and URLs.

Based on the action selected either 'Log and drop' or 'Log only' respective action is taken.

### Audit:

```
Navigate to Protect > Active threat response > MDR threat feeds  
  
Enable 'MDR threat feeds'  
  
Select the Action 'Log Only' or 'Log and drop'  
  
Log only: Only logs the threats.  
Log and drop: Logs and blocks threats.
```

### Remediation:

```
Navigate to Protect > Active threat response > MDR threat feeds  
  
Enable 'MDR threat feeds'  
  
Select the Action 'Log Only' or 'Log and drop'  
  
Log only: Only logs the threats.  
Log and drop: Logs and blocks threats.
```

### Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ConfigureFeeds/MDRThreatFeeds/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/Requirements/Licenses/index.html>
3. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ImplementFeeds/index.html>
4. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                        | IG 1                                                                                  | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.2 Collect Audit Logs</b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                        |    |    |    |
| v8               | <b>8.5 Collect Detailed Audit Logs</b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                       |  |  |
| v7               | <b>6.2 Activate audit logging</b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 Enable Detailed Logging</b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                       |  |  |

## *4.6 Ensure Third-party Threat Feeds is enabled (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Third party feed is a part of Active threat response feature on Sophos Firewall. It allows you to add threat intelligence from external threat feed sources to the firewall. The firewall automatically blocks traffic based on the IPv4 addresses, domains, and URLs listed in the feeds.

### **Rationale:**

Third party threat feed can be used to add additional custom threat feed to the firewall, which will monitor and respond by blocking the activities associated with them. The firewall automatically blocks traffic based on IPv4 addresses, domains and URLs listed in the feed



## Audit:

Navigate to Protect > Active threat response > Third-party feeds > Add

Select the Action either 'Block' or 'Monitor'

Indicator type from 'IPv4 address' , 'Domain' or 'URL'

Enter the 'External URL' where the threat feed file is hosted.

Under ' Authorization' select the authentication type to authorize the threat feed update.

Select 'Validate server certificate' if you want to validate the server certificate

Select the polling interval to synchronize the threat feed.

Click on 'Test Connection' to test the connection and then Save the configuration.

## Remediation:

Navigate to Protect > Active threat response > Third-party feeds > Add

Select the Action either 'Block' or 'Monitor'

Indicator type from 'IPv4 address' , 'Domain' or 'URL'

Enter the 'External URL' where the threat feed file is hosted.

Under ' Authorization' select the authentication type to authorize the threat feed update.

Select 'Validate server certificate' if you want to validate the server certificate

Select the polling interval to synchronize the threat feed.

Click on 'Test Connection' to test the connection and then Save the configuration.

## Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ConfigureFeeds/ThirdPartyThreatFeeds/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                               | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v8               | <b>8.2 <u>Collect Audit Logs</u></b><br>Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.                                                                                                                        |  |  |  |
| v8               | <b>8.5 <u>Collect Detailed Audit Logs</u></b><br>Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation. |                                                                                     |  |  |
| v7               | <b>6.2 <u>Activate audit logging</u></b><br>Ensure that local logging has been enabled on all systems and networking devices.                                                                                                                                                                         |  |  |  |
| v7               | <b>6.3 <u>Enable Detailed Logging</u></b><br>Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.                                                                                |                                                                                     |  |  |

## *4.7 Ensure NDR Essentials is enabled and configured (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

NDR Essentials is a cloud-hosted NDR solution that integrates directly with Sophos firewall. It uses advanced machine learning to detect threats in real-time without impacting the firewall's performance. This provides an additional layer of security in addition to existing firewall protection.

### **Rationale:**

NDR is designed to detect abnormal traffic patterns to help identify active adversaries on your network. Even skilled attackers need to move across or communicate out of your network to carry out an attack. NDR continuously monitors network traffic to detect suspicious activities that may be indicative of attacker activity.

### **Audit:**

Navigate to Protect > Active threat response > NDR Essentials.

Turn 'ON' NDR Essentials.

Interfaces > Select an 'Interface' so that NDR Essentials can identify new IoCs from the traffic flowing through them.

Select the 'Data center location' to which the traffic is sent for analysis. The default option is 'Let's Sophos Decide'.

Select the traffic's 'Minimum threat score' at which the firewall detects and logs threats. The default setting is High risk (Score 9 and 10) - Recommended

Under Actions, the option is set to 'Log' threats, because NDR Essentials currently only detects and logs threats.

Click on Apply

### **Remediation:**

Navigate to Protect > Active threat response > NDR Essentials.

Turn 'ON' NDR Essentials.

Interfaces > Select an 'Interface' so that NDR Essentials can identify new IoCs from the traffic flowing through them.

Select the 'Data center location' to which the traffic is sent for analysis. The default option is 'Let's Sophos Decide'.

Select the traffic's 'Minimum threat score' at which the firewall detects and logs threats. The default setting is High risk (Score 9 and 10) - Recommended

Under Actions, the option is set to Log threats, because NDR Essentials currently only detects and logs threats.

Click on Apply

**Default Value:**

By default, NDR Essential is not configured

**References:**

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ConfigureFeeds/NDREssentials/NDREssentialsConfigure/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/ActiveThreatResponse/ConfigureFeeds/NDREssentials/NDREssentialsAbout/index.html>

## **5 Protection Rules And Profiles**

This section covers all aspect of protection configuration both Ingress and Egress traffic including SSL/TLS Inspection rules, URL filtering, AV, IPS and Application control, Web server security profiles, Wireless and VPN profiles.

## *5.1 Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly. (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Configure Web Policy to control users' web browsing activities, block inappropriate web categories and enforce malware scanning for FTP and HTTP(S) traffic.

### **Rationale:**

Web protection keeps an organization safe from attacks that result from web browsing and helps you increase productivity. By blocking objectionable URL categories and potentially unwanted applications (PUAs), enforcing malware scanning for FTP, HTTP(S), the threat of malware propagation through the firewall is greatly reduced. It is recommended to mitigate malware found in FTP, HTTP(S) through outgoing traffic, you can configure to prevent users downloading certain File Types, Block web category or Warn with appropriate deterrent messages display to the users.

### **Impact:**

Any misconfigured policies or unintended exceptions will allow users to access inappropriate web categories, URLs that linked to drive-by-downloads and malware.

## Audit:

Navigate to `Protect > Web`.

Verify that configured web policies have categories with `objectionable classification` is set to block. Ensure that Status is set to `ON` with the block rule is on top.

Within the web policy `Advanced settings > Enable logging and reporting` is checked.

Navigate to `Protect > Web > General settings > Protection > Malware and content scanning`.

Verify that `Action on malware scan failure` is set to `Block(best protection)`.

Verify that `Block potentially unwanted applications` is checked.

Navigate to `Protect > Web > Exceptions`.

Verify that configured exceptions do not have dangerous `URL patterns, web site categories and wide range of destination IP address(website address)` that will have security impact to the `source IP addresses (end-users' address)` with skipped `HTTPS decryption, HTTPS certificate validation, malware and content scanning, Zero-day protection and policy check`.

## Remediation:

Navigate to `Protect > Web`

Set the web policy to block categories with `objectionable classification` and change the status to `ON`.

Within the web policy set the `Enable logging and reporting`.

Navigate to `Protect > Web > General settings > Protection > Malware and content scanning`

Action on `malware scan failure` is set to `Block(best protection)`.

Enable `Block potentially unwanted applications`.

Navigate to `Protect > Web > Exceptions`

Remove/edit `exceptions` with `URL patterns, website categories and destination IP address (website address)` that could reduce security effectiveness to the `source IP address (end-users' address)`.

## Default Value:

Not configured

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Web/WebGeneralSettings/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Web/Policies/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                     | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>8.7 Collect URL Request Audit Logs</b><br>Collect URL request audit logs on enterprise assets, where appropriate and supported.                                                                                                                                                                                                                                          |      |    |    |
| v8               | <b>9.3 Maintain and Enforce Network-Based URL Filters</b><br>Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets. |      |    |    |
| v7               | <b>7.4 Maintain and Enforce Network-Based URL Filters</b><br>Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.                                          |      |  |  |
| v7               | <b>7.5 Subscribe to URL-Categorization service</b><br>Subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default.                                                                                                                             |      |  |  |
| v7               | <b>7.6 Log all URL requests</b><br>Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.                                                                                                      |      |  |  |



## *5.2 Ensure SSL/TLS inspection rules is enabled to all relevant firewall policies (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

With SSL/TLS inspection rules, you can intercept and decrypt SSL and TLS connections over TCP, enabling Sophos Firewall to enforce secure connections between clients and web servers. SSL/TLS inspection enables the prevention of malware transmitted through encrypted connections.

### **Rationale:**

By applying SSL/TLS inspection rule to the applicable traffic, the threat of malware propagation through the encrypted communication is greatly reduced. SSL/TLS inspection profile also can limit any communication with insecure encryption protocol within the organization.

### **Impact:**

Not enforcing security policy on encrypted traffic may allow malware to transit the security boundary without blocks or alerts. With proper security policy to scan and decrypt the TLS/SSL traffic, Sophos Firewall has visibility of the communication and not only block the malware at the gateway but also preventing insecure communication to take place.

## Audit:

Navigate to `Protect > Rules and policies > SSL/TLS inspection rules > SSL/TLS inspection settings`.

Verify that `Non-decryptable traffic > SSL 2.0 and SSL 3.0` is set to `Reject` or `Drop`.

Verify that `SSL compression` is set to `Reject` or `Drop`.

Verify that `When SSL/TLS connections exceed limit` is set to `Drop` or `Reject`.

Verify that `TLS 1.3 decryption` is set to `Decrypt as 1.3`.

Verify that `Advanced settings > SSL/TLS engine` is set to `Enabled`.

Verify the configured `SSL/TLS inspection rule` and check the `Action` to `Decrypt` and `Log connections` is checked. The rule position should be above rules configured with `Action` set to `Don't decrypt`.

Verify the configured Firewall rules and `Scan HTTP and decrypted HTTPS` and `Use zero-day protection` is checked.

## Remediation:

Navigate to `Rules and policies > SSL/TLS inspection rules > SSL/TLS inspection settings`.

Set `Non-decryptable traffic > SSL 2.0 and SSL 3.0` to `Reject` or `Drop`.

Set `SSL compression` to `Reject` or `Drop`.

Set `When SSL/TLS connections exceed limit` to `Drop` or `Reject`.

Set `TLS 1.3 decryption` to `Decrypt as 1.3`.

Set `Advanced settings > SSL/TLS engine` to `Enabled`.

Navigate to configured `SSL/TLS inspection rule` and set the `Action` to `Decrypt` and `Log connections` is checked. Set the rule position to above rules configured with `Action` set to `Don't decrypt`.

Navigate to the configured Firewall rules. Set `Scan HTTP and decrypted HTTPS` and `Use zero-day protection` is checked.

### Default Value:

SSL/TLS inspection is enabled by default, but to decrypt the traffic, above configuration needs to be applied respectively.

### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/SSL/TLSInspectionRules/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/21.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/SSL/TLSInspectionRules/SSLTLSInspectionSettings/index.html#non-decryptable-traffic>

### CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

### 5.3 Ensure Application filter is set to block high risk (Risk Level 4 and 5) applications (Manual)

#### Profile Applicability:

- Level 2

#### Description:

When there is a firewall rule to allow outgoing traffic, configure it to identify and control Layer-7 applications and drop traffic that are classified under high risk applications (Risk Level 4 and 5) with application filter.

#### Rationale:

Most organizations may require visibility of the Layer-7 applications, and control access to applications for users behind the firewall. Application filter can reduce the attack surface of risk prone applications, peer-to-peer networking (P2P), these applications can be used to distribute bots, spyware, adware, trojans, rootkits, worms, and other types of malware. It is recommended to block traffic classified as high risk applications. Create custom policies according to the requirements of an organization.

#### Audit:

Navigate to `Rules and policies > Firewall rules`.

Verify that configured outgoing firewall rules with `Identify and control applications (App control)` is set to `Block high risk (Risk Level 4 and 5) apps`.

#### Remediation:

Navigate to `Rules and policies > Firewall rules`.

Set the configured outgoing firewall rules with `Identify and control applications (App control)` to `Block high risk (Risk Level 4 and 5) apps`.

#### Default Value:

Not enabled.

#### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Applications/HowToArticles/BlockApplicationsUsingApplicationFilter/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Applications/ApplicationFilter/index.html>

**CIS Controls:**

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## *5.4 Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Network attacks can be prevented using IPS rules. The firewall matches signatures with traffic patterns and takes the action specified in the rule. IPS signatures identify threats and specify a recommended action to take when the firewall encounters matching traffic. Signatures are specific to applications, services, or platforms. The firewall includes predefined signatures and you can also create custom signatures.

### **Rationale:**

Sophos firewall intercepts and blocks network based attacks targeted at both servers and clients protected behind the firewall. The set of default policies prevents network attacks for several common types of traffic. Depending on the traffic requirement, custom IPS rules can be created to take specific actions based on severity, target, platform and category.

## Audit:

Navigate to `Rules and policies > Firewall rules`.

Navigate to configured firewall rules. Verify that `Detect and prevent exploits (IPS)` is configured with appropriate IPS rule based on the direction of the traffic. Either one of these rule should be present generalpolicy, lantowan\_strict, lantowan\_general, dmzpolicy, LAN TO WAN, LAN TO DMZ, WAN TO DMZ, WAN TO LAN, DMZ TO WAN, DMZ TO LAN or "custom IPS rule".

It's recommended to have IPS rule with client-side exploitation protection policy for user network with allowed outgoing. And similar policy with server side protection for any incoming firewall rules from WAN zone.

## Remediation:

Navigate to 'Protect > Intrusion prevention > IPS policies > Enable IPS protection'

Navigate to `Rules and policies > Firewall rules`.

Navigate to configured firewall rules. Set `Detect and prevent exploits (IPS)` with appropriate IPS rule based on the direction of the traffic. Configure IPS policy with generalpolicy, lantowan\_strict, lantowan\_general, dmzpolicy, LAN TO WAN, LAN TO DMZ, WAN TO DMZ, WAN TO LAN, DMZ TO WAN, DMZ TO LAN or "custom IPS rule".

Set IPS rule with client-side exploitation protection policy for user network with outgoing allowed. And similar policy with server side protection for any incoming firewall rules from WAN zone.

## Default Value:

By default IPS is turned off

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/IntrusionPrevention/IPSPolicies/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                             | IG 1 | IG 2 | IG 3                                                                                  |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|---------------------------------------------------------------------------------------|
| v8               | <b>13.8 Deploy a Network Intrusion Prevention Solution</b><br>Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service. |      |      |  |

| Controls Version | Control                                                                                                                                                                                                                         | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v7               | <p><b>12.7 <u>Deploy Network-Based Intrusion Prevention Systems</u></b></p> <p>Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.</p> |      |      | ●    |



## *5.5 Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Sophos firewall protects web servers against Layer 7 (application) vulnerability exploits. These attacks include cookie, URL, and form manipulation. It can also mitigate common threats such as application and cross-site scripting (XSS) attacks. Sophos firewall provides default policies for some common web services.

### **Rationale:**

Sophos firewall's Web Application Firewall (WAF) feature protects web servers deployed in a network and related applications from any underlying vulnerability exploits. It protects applications accessed via HTTP and HTTPS at the layer-7 Application Layer. Besides Layer 7 based attacks, the web server is safeguarded against cookie tampering, forceful browsing, and hidden field tampering. The WAF also mitigates user-induced vulnerabilities in applications that leave web applications open to attacks, such as cross-site scripting, directory traversal, and forced URL browsing.

## Audit:

Navigate to `Protect > Web server > General settings > SlowHTTP protection settings`.

Verify that `Time-out for request headers` is `ON`.

Verify the minimum amount of time to receive a request `Soft limit` is set to optimal configuration. Default setting is `10`.

Verify the maximum amount of time to receive the request header `Hard limit` is set to optimal configuration. Default setting is `30`.

Verify the amount of data, in bytes, to extend the time-out set by the soft limit. Every time the rate is exceeded, the soft limit is increased by one second. The default extension rate is `5000`.

Verify that `TLS version settings > TLS version` is set to TLS 1.2. Select the minimum TLS version that is allowed to connect to the WAF. Note that if TLS version 1.2 is selected, clients like Microsoft Internet Explorer 8 or earlier and those running on Window XP won't be able to connect to the WAF.

Navigate to the configure WAF rules `Rules and policies > Firewall rules`, filter `Rule type > WAF`. Verify under `Advanced > Protection > edit protection policy` to check `Mode` is set to `Reject`.

Verify that `Cookie signing` is set to `ON`.

Verify that `Static URL hardening` is set to `ON` with specify the URLs you want to serve. Note that this feature isn't effective for dynamic URLs created by the client, for example, using JavaScript.

Verify that `Form hardening` is set to `ON`.

Verify that `Antivirus` is set to `ON` with `Mode` set to either `Sophos` or `Dual scan`. And Direction of the scanning is set to `Uploads and Downloads`.

Verify that `Block unscannable content` is set to `ON`.

Verify that `Block clients with bad reputation` is set to `ON`.

Verify that `Common threat filter` is set to `ON`. And confirm that these rule IDs  
(901100,901110,949100,949190,949110,959100,980100,980110,980120,980130,980140)  
) are not added to the Skip filter rules.

Verify that `Application attacks` is checked.

Verify that `SQL injection attacks` is checked.

Verify that `XSS attacks` is checked.

Verify that `Protocol enforcement` is checked.

Verify that `Scanner detection` is checked.

Verify that `Data leakage` is checked.

Verify that 'HTTP Strict Transport Security' is checked to make sure your site is accessed using only HTTPS.

Enable 'MIME-type sniffing protection' to instruct the browser to use the MIME type indicated in the web server's response

Within the configured firewall rule with WAF verify that Intrusion prevention is set to either `WAN TO LAN` or `WAN TO DMZ` or custom IPS rule with target server platform.

To Enforce MFA for WAF-protected web servers

Navigate to 'Configure' > 'Authentication' > 'Multi-factor Authentication' > 'MFA Settings' > Select 'All users' or 'Specific users and groups'

Turn 'ON' Generate OTP token with next sign-in if Users must use an authentication application for generating passcodes OR Keep if 'OFF' if users must use hardware token.

Enable Require MFA for 'Web application firewall'

In the authentication policy where MFA needs to be enforced. Navigate to 'Protect' > 'Web Server' > 'Authentication Policies' > Edit the policy to set the client Mode to 'Form' and select an 'Authentication template' and 'Users or groups'.

In the WAF rule to enforce MFA, select the Web Server and Authentication policy

## Remediation:

Navigate to `Protect > Web server > General settings > SlowHTTP protection settings`.

Set `Time-out for request headers` to `ON`.

Set the minimum amount of time to receive a request `Soft limit` to optimal configuration. Default setting is `10`.

Set the maximum amount of time to receive the request header `Hard limit` to optimal configuration. Default setting is `30`.

Set the amount of data, in bytes, to extend the time-out set by the soft limit. Every time the rate is exceeded, the soft limit is increased by one second. The default extension rate is `5000`.

Set `TLS version settings > TLS version` to TLS 1.2. Select the minimum TLS version that is allowed to connect to the WAF. Note that if TLS version 1.2 is selected, clients like Microsoft Internet Explorer 8 or earlier and those running on Window XP won't be able to connect to the WAF.

Navigate to the configure WAF rules `Rules and policies > Firewall rules`, filter `Rule type > WAF`. Under `Advanced > Protection > edit protection policy` set `Mode` to `Reject`.

Set `Cookie signing` to `ON`.

Set `Static URL hardening` to `ON` with specify the URLs you want to serve. Note that this feature isn't effective for dynamic URLs created by the client, for example, using JavaScript.

Set `Form hardening` to `ON`.

Set `Antivirus` to `ON` with scanning `Mode` to either `Sophos` or `Dual scan`. And Direction of the scanning is set to `Uploads and Downloads`.

Set `Block unscannable content` to `ON`.

Set `Block clients with bad reputation` to `ON`.

Set `Common threat filter` to `ON`. Remove these rule IDs (901100,901110,949100,949190,949110,959100,980100,980110,980120,980130,980140) added to the Skip filter rules.

Set `Application attacks` to enable.

Set `SQL injection attacks` to enable.

Set `XSS attacks` to enable.

Set `Protocol enforcement` to enable.

Set `Scanner detection` to enable.

Set `Data leakage` to enable.

Verify that 'HTTP Strict Transport Security' is checked to make sure your site is accessed using only HTTPS.

Enable 'MIME-type sniffing protection' to instruct the browser to use the MIME type indicated in the web server's response

Within the configured firewall rule with WAF verify that Intrusion prevention is set to either `WAN TO LAN` or `WAN TO DMZ` or custom IPS rule with target server platform.

To Enforce MFA for WAF-protected web servers

Navigate to 'Configure' > 'Authentication' > 'Multi-factor Authentication' > 'MFA Settings' > Select 'All users' or 'Specific users and groups'

Turn 'ON' Generate OTP token with next sign-in if Users must use an authentication application for generating passcodes OR Keep if 'OFF' if users must use hardware token.

Enable Require MFA for 'Web application firewall'

In the authentication policy where MFA needs to be enforced. Navigate to 'Protect' > 'Web Server' > 'Authentication Policies' > Edit the policy to set the client Mode to 'Form' and select an 'Authentication template' and 'Users or groups'.

In the WAF rule to enforce MFA, select the Web Server and Authentication policy

### Default Value:

Not configured.

### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/WebServer/ProtectionPolicies/WAFProtectionPolicyAdd/index.html>
2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/WebServer/WebServers/WAFWebServerAdd/index.html>
3. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/WebServerProtection/WAF/Rules/index.html>
4. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/WebServerProtection/WAF/Rules/index.html>
5. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/OneTimePassword/AuthenticationMFASettings/index.html#services-requiring-mfa>

### CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                   | IG 1 | IG 2 | IG 3 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|------|
| v8               | <b>13.10 Perform Application Layer Filtering</b><br>Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.                                       |      |      | ●    |
| v7               | <b>9.5 Implement Application Firewalls</b><br>Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged. |      |      | ●    |

## *5.6 Ensure Email protection is configured with appropriate protection policies (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Create one or more Email protection policy to handle email routing and protect domains and mail servers. You can configure SMTP/S, POP/S, and IMAP/S policies with SPAM and malware checks, data protection, and Email encryption.

### **Rationale:**

By scanning both inbound and outbound Email traffic, the threat of malware delivered through Emails and data exfiltration can be prevented at the gateway firewall. Per domain policy allows unrestricted configuration based on security needs. Appropriate Email protection policy enforces TLS, SMTP DoS and other security settings for incoming and outgoing emails.

## Audit:

Navigate to `Protect > Email > General settings`. Verify that appropriate `SMTP deployment mode` is used. Note that `legacy mode` is not compatible with Zero-day protection for Email.

Navigate to `SMTP settings`.

Verify that `Reject based on IP reputation`. Sophos Firewall checks the sender's IP reputation before the spam checks specified in the SMTP policy.

Verify that `SMTP DoS settings` is Enable. Sophos Firewall protects the network from SMTP denial-of-service attacks.

Navigate to `SMTP TLS configuration`. Verify that `Disable legacy TLS protocols` is Enable. To overcome TLS vulnerabilities, it is recommended to turn off legacy TLS protocols.

Navigate to `POP and IMAP TLS configuration`. Verify that `Disable legacy TLS protocols` is Enable.

Navigate to `Malware protection`. Verify that `Primary antivirus engine` is set to `Sophos`. If `Avira` is selected Sophos Firewall will turn off Sandstorm in SMTP policies with single antivirus scan.

Navigate to `DKIM verification`. Verify that DKIM verification is `ON` and `DKIM verification failed`, `Invalid DKIM signature`, `No DKIM signature found` should be set to `Quarantine` or `Reject`. With DKIM the firewall validates the source domain name and message integrity through cryptographic authentication, preventing email spoofing. DKIM verification is applied to inbound emails. Note that Sophos Firewall quarantines DKIM-signed emails that use RSA SHA-1 or have key length less than 1024 or more than 2048 bits.

Navigate to `Protect > Email > Relay settings > Host based relay`. Verify that `ANY` is not added to the `allow relay from hosts/networks`. Adding `ANY` will result in an open relay, allowing anyone on the internet to send emails through Sophos Firewall.

Navigate to `Protect > Email > Policy & exceptions`. Verify the configured SMTP policy `Malware protection > Selected antivirus action` is set to `Drop` and `Quarantine unscannable content` is checked and `Use zero-day protection` is enabled.

## Remediation:

Navigate to `Protect > Email > General settings`. Set the appropriate `SMTP deployment mode` to `MTA mode` when possible. `legacy mode` is not compatible with Zero-day protection for Email and reduce the security effectiveness.

Navigate to `SMTP settings`.

Set `Reject based on IP reputation` to Enable. Sophos Firewall checks the sender's IP reputation before the spam checks specified in the SMTP policy.

Set `SMTP DoS settings` to Enable. Sophos Firewall protects the network from SMTP denial-of-service attacks.

Navigate to `SMTP TLS configuration`. Set `Disable legacy TLS protocols` to Enable. To overcome TLS vulnerabilities, it is recommended to turn off legacy TLS protocols.

Navigate to `POP and IMAP TLS configuration`. Set `Disable legacy TLS protocols` to Enable.

Navigate to `Malware protection`. Set `Primary antivirus engine` to `Sophos`. If `Avira` is selected Sophos Firewall will turn off Zero-day protection in SMTP policies with single antivirus scan.

Navigate to `DKIM verification`. Set `DKIM verification` to `ON` and `DKIM verification failed`, `Invalid DKIM signature`, `No DKIM signature found` are set to `Quarantine` or `Reject`. With DKIM the firewall validates the source domain name and message integrity through cryptographic authentication, preventing email spoofing. DKIM verification is applied to inbound emails. Note that Sophos Firewall quarantines DKIM-signed emails that use RSA SHA-1 or have key length less than 1024 or more than 2048 bits.

Navigate to `Protect > Email > Relay settings > Host based relay`. Remove `ANY` from the `allow relay from hosts/networks`. Adding `ANY` will result in an open relay, allowing anyone on the internet to send emails through Sophos Firewall. Set only the specified host or enable authenticated relay.

Navigate to `Protect > Email > Policy & exceptions`. Set the configured SMTP policy `Malware protection > Selected antivirus action` to `Drop` and `Quarantine unscannable content` is checked and `Use zero-day protection` is enabled.

### **Default Value:**

Not configured.

### **References:**

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Email/GeneralSettings/index.html>



2. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Email/PoliciesExceptions/EmailSMTPRouteAndScanPolicyAdd/index.html>

**CIS Controls:**

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## *5.7 Ensure DoS & Spoof Protection is enabled with the appropriate settings (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Enable SYN/TCP/UDP Flood protection for source and destination networks with appropriate threshold for Flood protection which depend highly on the environment and device used. Default packet/minutes or packet/seconds value may not be appropriate for all the environment and understanding of traffic patterns on the specific environment may be required to set accurate threshold.

Enable Spoof protection to drop the packet if the source IP address of a packet does not match any entry on the firewall's routing table or if the packet is not from a direct subnet.

### **Rationale:**

DoS/DDoS attacks where the CPU and memory buffers of the victim device becomes overwhelmed by incomplete sessions. Many attacks can be successfully mitigated against resources protected by firewall or firewall itself.

### **Impact:**

Organization may expose to both internal and external DoS and reconnaissance attacks. Malicious traffic flooding and malware communication can cause network congestion and consuming valuable network resources.

## Audit:

Navigate to `Protect > Intrusion Prevention > DoS & Spoof Protection`  
Verify that `Enable spoof prevention` is checked on LAN and DMZ zones.

Under DoS settings > Verify that `Apply Flag` is checked on `SYN flood`, `UDP flood`, `TCP flood`, `ICMP/ICMPv6` flood on both Source and Destination.

Under DoS settings > Verify that `Apply Flag` is checked on `Dropped source routed packets`, `Disable ICMP/ICMPv6 redirect packet`, `ARP hardening` on Destination.

Verify that `DoS bypass rule` is not added with wide range of source or destination networks that will reduce integrity of overall DoS protection.

## Remediation:

Navigate to `Protect > Intrusion Prevention > DoS & Spoof Protection`  
Set `Enable spoof prevention` is checked on LAN and DMZ zones.

Under DoS settings > Set `Apply Flag` is checked on `SYN flood`, `UDP flood`, `TCP flood`, `ICMP/ICMPv6` flood on both Source and Destination.

Under DoS settings > Set `Apply Flag` is checked on `Dropped source routed packets`, `Disable ICMP/ICMPv6 redirect packet`, `ARP hardening` on Destination.

Validate `DoS bypass rule` is not added with wide range of source or destination networks that will reduce integrity of overall DoS protection.

## Default Value:

Not Configured.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/IntrusionPrevention/DoSSpoofProtection/index.html>

## CIS Controls:

| Controls Version | Control                                                   | IG 1 | IG 2 | IG 3 |
|------------------|-----------------------------------------------------------|------|------|------|
| v8               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |
| v7               | 0.0 <u>Explicitly Not Mapped</u><br>Explicitly Not Mapped |      |      |      |

## *5.8 Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Window service ports directly accessible from WAN zone could lead to bruteforce attempts, wormable attacks and other unpatched vulnerabilities.

Unencrypted protocols that could potentially impact confidentiality, integrity and availability shouldn't be directly accessible from the WAN Zone.

### **Rationale:**

Any allowed rules with port-forwarding (DNAT) enabled to access internal Window services such as (TCP/UDP 445,137-139,3389) and other unencrypted protocols (TCP/UDP 21,23,113,135,513,389,1433,5800,5900) could lead to potential compromise or data leakage.

### **Impact:**

Directly accessible ports to the internal servers open bigger attack surface for the adversary. For example, allowing Port 3389 RDP from internet could lead to unpatched vulnerability such as Bluekeep CVE-2019-0708, vulnerability known to associate with WannaCry ransomware.

### **Audit:**

```
Navigate to `Rules and policies > Firewall rules`.
Verify the `Firewall rules` with `Source zone` `WAN` with service ports
`TCP/UDP 445,137-139,3389,21,79,23,113,135,513,389,1433,5800,5900` exists in
the allowed rules.
```

### **Remediation:**

```
Navigate to `Rules and policies > Firewall rules`.
Disable or only allow with specific source IP address in `Firewall rules`
with `Source zone` `WAN` with service ports `TCP/UDP 445,137-
139,3389,21,79,23,113,135,513,389,1433,5800,5900`. When absolute necessary to
allow access from Internet, consider the use of VPN.
```

### **Default Value:**

Not Configured.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/index.html#server-access-assistant-dnat>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                                                                                                                                              | IG 1                                                                                | IG 2                                                                                  | IG 3                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.                                                                                                                                                         |  |    |    |
| v8               | <b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b><br>Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.                                                                                                                         |  |    |    |
| v8               | <b>7.5 <u>Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b><br>Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.                                                                                      |                                                                                     |  |  |
| v8               | <b>7.6 <u>Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b><br>Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.                                                                                                            |                                                                                     |  |  |
| v8               | <b>13.5 <u>Manage Access Control for Remote Assets</u></b><br>Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date. |                                                                                     |  |  |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                                                                                                                                                         |                                                                                     |  |  |
| v7               | <b>12.2 <u>Scan for Unauthorized Connections across Trusted Network Boundaries</u></b><br>Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.                                                                                                                                                          |                                                                                     |  |  |

## *5.9 Ensure Wireless Protection is configured with secure configuration (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

When Sophos firewall is used as Wireless controller to manage Sophos Access Points, it is important to tighten configuration to prevent unauthorized access to the Wireless network.

### **Rationale:**

By providing wireless connectivity to the clients, it creates potential attack surface to the wireless users as well as the local network. Important configurations such as security mode, method of handling traffic should be considered before providing the Wireless access.

### **Impact:**

Authentication with weaker encryption algorithm could lead to compromising encryption keys and unauthorized access to both Wireless and local network. Due to availability and lack of physical access control to Wireless network, it is important to tighten security settings.

## Audit:

Navigate to `Protect > Wireless > Wireless networks`  
Verify the existing `Wireless` settings with `Security mode`, either `WPA2 Personal` or `WPA2 Enterprise` should be used.

Under `Advanced settings`  
Verify that `Encryption` is set to `AES[secure]`  
Verify that `Time-based access` is `Enable` with `Select active time` and appropriate schedule to limit the availability.

Verify that `Client isolation` is `Enabled`.

## Remediation:

Navigate to `Protect > Wireless > Wireless networks`  
Set the existing `Wireless` settings with `Security mode`, either `WPA2 Personal` or `WPA2 Enterprise`.

Under `Advanced settings`  
Set `Encryption` to `AES[secure]`  
Set `Time-based access` to `Enable` with `Select active time` and configure appropriate schedule to limit the availability.

Set `Client isolation` to `Enabled`.

## Default Value:

Not Configured.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Wireless/WirelessNetworks/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                            | IG 1 | IG 2                                                                                  | IG 3                                                                                  |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| v8               | <b>3.10 <u>Encrypt Sensitive Data in Transit</u></b><br>Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).                                                                    |      |  |  |
| v8               | <b>4.8 <u>Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u></b><br>Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function. |      |  |  |

| Controls Version | Control                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                | IG 3                                                                                |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| v7               | <u>15.6 Disable Peer-to-peer Wireless Network Capabilities on Wireless Clients</u><br>Disable peer-to-peer (ad hoc) wireless network capabilities on wireless clients.       |                                                                                     |  |  |
| v7               | <u>15.7 Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data</u><br>Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit. |  |  |  |



## 5.10 Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone (Manual)

### Profile Applicability:

- Level 1

### Description:

Allowed firewall rules with no specific source or ANY service definitions from WAN/untrusted zone could lead to unintended exposure to the outside threats.

### Rationale:

Limit the unintended exposure to systems and services. Allowed rules from WAN zone should be created with very specific source network or GEO IP and targeted service definition to the internal host.

On top of the allowed policy, there should be IPS rule enabled with WAN to LAN or WAN to DMZ profile.

### Impact:

Having a allowed firewall rule 'ANY' to 'ANY' with no layer-7 threats protections could lead to threat exposure of unpatched systems, bruteforce attempts and denial of service etc.

### Audit:

```
Navigate to `Protect > Rules and policies > Firewall rules`.
Filter `Destination zone` to `LAN` or `DMZ`.
```

```
Verify that no allowed firewall rules from `WAN` zone with service definition
`ANY` to `LAN` or `DMZ` zone with destination network set to `ANY`.
```

### Remediation:

```
Navigate to `Protect > Rules and policies > Firewall rules`.
Filter `Destination zone` to `LAN` or `DMZ`.
```

```
Remove allowed firewall rules from `WAN` zone with service definition `ANY`
to `LAN` or `DMZ` zone with destination network set to `ANY`. Or change the
rule to specific source/destination with target service definition.
```

### Default Value:

Not Configured.

## References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/RulesAndPolicies/FirewallRules/index.html>

## CIS Controls:

| Controls Version | Control                                                                                                                                                                                                                                                                      | IG 1                                                                                | IG 2                                                                                 | IG 3                                                                                 |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| v8               | <b>4.4 <u>Implement and Manage a Firewall on Servers</u></b><br>Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.                                 |  |   |   |
| v8               | <b>4.5 <u>Implement and Manage a Firewall on End-User Devices</u></b><br>Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. |  |   |   |
| v7               | <b>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></b><br>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.                                                 |                                                                                     |  |  |

## 5.11 Ensure a Optimal Firewall health check score (Manual)

### Profile Applicability:

- Level 2

### Description:

Health check feature provides quick visibility into the overall security readiness and hygiene of the firewall deployment. It highlights the missing configurations, shows which issues are high, medium or low impact to prioritize them.

### Rationale:

Firewall Health Check identifies gaps in protection by highlighting the missing configurations that can be exploited by threat actors. It enhances operational efficiency by centralizing health insights in one dashboard and improves security posture by guiding the admins to enable recommended controls based on best practices.

### Audit:

Navigate to ' Monitor & Analyze' > 'Firewall Health check'

Policy compliance shows you the Compliant and Non-compliant status.

It shows Compliant or Non-Compliant Status for Individual Policies.

Under 'Action ' for Non-Compliant policy, select ' Fix '. This navigates you to configuration page for that control.

### Remediation:

Navigate to ' Monitor & Analyze' > 'Firewall Health check'

Policy compliance shows you the Compliant and Non-compliant status.

It shows Compliant or Non-Compliant Status for Individual Policies.

Under 'Action ' for Non-Compliant policy, select ' Fix '. This navigates you to configuration page for that control.

### References:

1. <https://docs.sophos.com/nsg/sophos-firewall/22.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/FirewallHealthCheck/index.html>

## 5.12 Ensure Sophos DNS protection is configured (Manual)

### Profile Applicability:

- Level 2

### Description:

Sophos DNS protection is a cloud-based service that blocks access to malicious or unwanted domains using real-time threat intelligence from SophosLabs. This method provides enhanced web security without requiring a third-party DNS solution.

### Rationale:

Sophos DNS protection adds another layer of security to every network. it complements the protection provided by the other security features of Sophos Firewall. Deploying it on a network protected by the firewall ensures all protocols, ports are protected against risky or inappropriate domains.

### Audit:

To use DNS protection in Sophos Firewall, the firewall should be connected to and managed by Sophos Central.

There are two parts to configure the DNS protection

1. Sophos Central Configuration.
2. Sophos Firewall configuration.

#### 1.Sophos Central configuration,

Login to Sophos Central Dashboard to which the firewall is registered and managed from. Navigate to 'My Products' > 'DNS Protection' > 'Locations' > Click on 'Add' > Enter the name and description for the location > In 'IPv4 addresses or FQDNs' > Add the firewall WAN Interface IP or the firewall hostname registered with DDNS providers > Click on 'Save.'

In Sophos Central, copy the DNS Protection IP addresses; these IP addresses need to be configured in Sophos Firewall to be use DNS Protection. To copy the DNS Protection IP address, navigate to 'My Products ' > ' DNS Protection ' > ' Installers ' > Next to IP addresses, click 'Copy.'

#### 2. Sophos Firewall Configuration

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'IPv4' > 'Static DNS' > In 'DNS 1' enter one of the IP addresses copied from Sophos Central to be used as a primary DNS Protection Server. > In 'DNS 2' enter the other IP addresses copied from Sophos Central to be used as a secondary DNS Protection Server. We recommend you don't add any other DNS server in DNS 3. If the firewall switches to the third DNS server, you will lose the protection offered by DNS protection.

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'IPv6' > 'Static DNS' > Leave DNS 1 , DNS 2, DNS 3 blank

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'DNS query configuration' > Select 'Choose IPv4 DNS Server over IPv6'

Click 'Apply'

Setup network devices to use Sophos Firewall as the DNS resolver. Update the firewall DHCP Server so that the network devices use the firewall as the DNS resolver.

Navigate to 'Configure' > 'Network' > 'DHCP' > Under 'Server' select the configured DHCP server and Click on 'Edit' > In 'Interface', make note of the selected DHCP Interface's IP address > 'DNS Server' > Unselect 'Use device's DNS settings' > 'Primary DNS' , enter the IP address of the DHCP interface noted in the above > 'Secondary DNS', enter the Public IP address of the DNS protection obtained from Sophos Central in the above step > Click 'Save' Repeat these steps for all the configured DHCP servers in the firewall

## **Remediation:**

To use DNS protection in Sophos Firewall, the firewall should be connected to and managed by Sophos Central.

There are two parts to configure the DNS protection

1. Sophos Central Configuration.
2. Sophos Firewall configuration.

### **1.Sophos Central configuration,**

Login to Sophos Central Dashboard to which the firewall is registered and managed from. Navigate to 'My Products' > 'DNS Protection' > 'Locations' > Click on 'Add' > Enter the name and description for the location > In 'IPv4 addresses or FQDNs' > Add the firewall WAN Interface IP or the firewall hostname registered with DDNS providers > Click on 'Save.'

In Sophos Central, copy the DNS Protection IP addresses; these IP addresses need to be configured in Sophos Firewall to be use DNS Protection. To copy the DNS Protection IP address, navigate to 'My Products' > 'DNS Protection' > 'Installers' > Next to IP addresses, click 'Copy.'

### **2. Sophos Firewall Configuration**

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'IPv4' > 'Static DNS' > In 'DNS 1' enter one of the IP addresses copied from Sophos Central to be used as a primary DNS Protection Server. > In 'DNS 2' enter the other IP addresses copied from Sophos Central to be used as a secondary DNS Protection Server. We recommend you don't add any other DNS server in DNS 3. If the firewall switches to the third DNS server, you will lose the protection offered by DNS protection.

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'IPv6' > 'Static DNS' > Leave DNS 1 , DNS 2, DNS 3 blank

Navigate to 'Configure' > 'Network' > 'DNS' > 'DNS Configuration' > 'DNS query configuration' > Select 'Choose IPv4 DNS Server over IPv6'

Click 'Apply'

Setup network devices to use Sophos Firewall as the DNS resolver. Update the firewall DHCP Server so that the network devices use the firewall as the DNS resolver. Navigate to 'Configure' > 'Network' > 'DHCP' > Under 'Server' select the configured DHCP server and Click on 'Edit' > In 'Interface', make note of the selected DHCP Interface's IP address > 'DNS Server' > Unselect 'Use device's DNS settings' > 'Primary DNS' , enter the IP address of the DHCP interface noted in the above > 'Secondary DNS', enter the Public IP address of the DNS protection obtained from Sophos Central in the above step > Click 'Save' Repeat these steps for all the configured DHCP servers in the firewall

### **Default Value:**

By default DNS protection in Sophos Firewall is not configured

### **References:**

1. <https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/DNSProtection/NetworkSetup/ConfigureSophosFirewallToUseDNSProtection/index.html>

# Appendix: Summary Table

| CIS Benchmark Recommendation |                                                                                                                    | Set Correctly            |                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                    | Yes                      | No                       |
| <b>1</b>                     | <b>Device Setup And Administration</b>                                                                             |                          |                          |
| <b>1.1</b>                   | <b>General Settings</b>                                                                                            |                          |                          |
| 1.1.1                        | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in (Automated)              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.2                        | Ensure login disclaimer is set (Automated)                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3                        | Ensure NTP servers are configured appropriately (Manual)                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4                        | Ensure SSL server certificate for remote SSL VPN is configured correctly (Manual)                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5                        | Ensure password complexity check is enabled (Automated)                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6                        | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7                        | Ensure valid certificate is set for web browser used to access Webadmin interface (Manual)                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.8                        | Ensure MFA for Web console access and remote access VPN (Manual)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.9                        | Ensure MFA for default admin (Manual)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.10                       | Set Hostname (Automated)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>1.2</b>                   | <b>SNMP &amp; Device Notification Settings</b>                                                                     |                          |                          |
| 1.2.1                        | Ensure SNMPv3 is selected for queries and traps (Automated)                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2                        | Ensure notification is configured to send system and security events (Manual)                                      | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                                                                             | Set Correctly            |                          |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                                             | Yes                      | No                       |
| <b>2</b>                     | <b>User Identification &amp; Authentication</b>                                                                                                             |                          |                          |
| 2.1                          | Ensure Firewall rules are configured to identify users before authorizing access (Manual)                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2                          | Ensure Encrypted connection is used in connecting external Active Directory and LDAP (Manual)                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>3</b>                     | <b>System Services, Firmware and Updates</b>                                                                                                                |                          |                          |
| 3.1                          | Ensure "Fully Synchronized" High Availability peer is configured (Manual)                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2                          | Ensure 'Pattern updates' is set to download and install updates every 15 minutes (Automated)                                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3                          | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes' (Manual)                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4                          | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency (Manual)                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5                          | Ensure No Expired Subscription Licenses (Manual)                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6                          | Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode" (Manual)                                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7                          | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server (Manual)                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>4</b>                     | <b>Advanced Threat &amp; Synchronized Security</b>                                                                                                          |                          |                          |
| 4.1                          | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop' (Manual)                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2                          | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |



| CIS Benchmark Recommendation |                                                                                                                                       | Set Correctly            |                          |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                                                       | Yes                      | No                       |
| 4.3                          | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode (Manual)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4                          | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules (Manual)                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5                          | Ensure MDR Threat Feeds is enabled (Manual)                                                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6                          | Ensure Third-party Threat Feeds is enabled (Manual)                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7                          | Ensure NDR Essentials is enabled and configured (Manual)                                                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| <b>5</b>                     | <b>Protection Rules And Profiles</b>                                                                                                  |                          |                          |
| 5.1                          | Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly. (Manual)           | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.2                          | Ensure SSL/TLS inspection rules is enabled to all relevant firewall policies (Manual)                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.3                          | Ensure Application filter is set to block high risk (Risk Level 4 and 5) applications (Manual)                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4                          | Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules (Manual)                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.5                          | Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use (Manual)         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.6                          | Ensure Email protection is configured with appropriate protection policies (Manual)                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.7                          | Ensure DoS & Spoof Protection is enabled with the appropriate settings (Manual)                                                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8                          | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |

| CIS Benchmark Recommendation |                                                                                                          | Set Correctly            |                          |
|------------------------------|----------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                              |                                                                                                          | Yes                      | No                       |
| 5.9                          | Ensure Wireless Protection is configured with secure configuration (Manual)                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10                         | Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone (Manual) | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.11                         | Ensure a Optimal Firewall health check score (Manual)                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.12                         | Ensure Sophos DNS protection is configured (Manual)                                                      | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9            | Ensure Wireless Protection is configured with secure configuration                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3          | Ensure NTP servers are configured appropriately                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4          | Ensure SSL server certificate for remote SSL VPN is configured correctly                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7          | Ensure valid certificate is set for web browser used to access Webadmin interface                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1          | Ensure SNMPv3 is selected for queries and traps                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure Encrypted connection is used in connecting external Active Directory and LDAP                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode"                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8            | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9            | Ensure Wireless Protection is configured with secure configuration                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10           | Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3          | Ensure NTP servers are configured appropriately                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4          | Ensure SSL server certificate for remote SSL VPN is configured correctly                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7          | Ensure valid certificate is set for web browser used to access Webadmin interface                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1          | Ensure SNMPv3 is selected for queries and traps                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure Encrypted connection is used in connecting external Active Directory and LDAP                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode"                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'          | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4            | Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.5            | Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8            | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9            | Ensure Wireless Protection is configured with secure configuration                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10           | Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v7 Unmapped Recommendations

| Recommendation |                                                         | Set Correctly            |                          |
|----------------|---------------------------------------------------------|--------------------------|--------------------------|
|                |                                                         | Yes                      | No                       |
| 1.1.8          | Ensure MFA for Web console access and remote access VPN | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.9          | Ensure MFA for default admin                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.10         | Set Hostname                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7            | Ensure NDR Essentials is enabled and configured         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.11           | Ensure a Optimal Firewall health check score            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.12           | Ensure Sophos DNS protection is configured              | <input type="checkbox"/> | <input type="checkbox"/> |



# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7          | Ensure valid certificate is set for web browser used to access Webadmin interface                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1          | Ensure SNMPv3 is selected for queries and traps                                                                                                    | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                                              | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                              | Set Correctly            |                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                              | Yes                      | No                       |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                   | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8            | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10           | Ensure No Firewall Rules with source `ANY`, service `ANY` and destination `ANY` from `WAN` Zone                              | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3          | Ensure NTP servers are configured appropriately                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4          | Ensure SSL server certificate for remote SSL VPN is configured correctly                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7          | Ensure valid certificate is set for web browser used to access Webadmin interface                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1          | Ensure SNMPv3 is selected for queries and traps                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure notification is configured to send system and security events                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure Encrypted connection is used in connecting external Active Directory and LDAP                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode"                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8            | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9            | Ensure Wireless Protection is configured with secure configuration                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10           | Ensure No Firewall Rules with source 'ANY', service 'ANY' and destination 'ANY' from 'WAN' Zone                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

| Recommendation |                                                                                                                                  | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                  | Yes                      | No                       |
| 1.1.1          | Ensure admin session 'logout' for inactivity and 'block' is configured for failed sign-in                                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.3          | Ensure NTP servers are configured appropriately                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.4          | Ensure SSL server certificate for remote SSL VPN is configured correctly                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.5          | Ensure password complexity check is enabled                                                                                      | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.6          | Ensure management access to the device is restricted from selected IP addresses and disable from WAN Zone                        | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.7          | Ensure valid certificate is set for web browser used to access Webadmin interface                                                | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.1          | Ensure SNMPv3 is selected for queries and traps                                                                                  | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.2.2          | Ensure notification is configured to send system and security events                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.1            | Ensure Firewall rules are configured to identify users before authorizing access                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 2.2            | Ensure Encrypted connection is used in connecting external Active Directory and LDAP                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.2            | Ensure 'Pattern updates' is set to download and install updates every 15 minutes                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.3            | Ensure 'Hotfix' is set to 'Allow Automatic Installation of hotfixes'                                                             | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.4            | Ensure Sophos Firewall takes encrypted backup of the configuration and send to designated email address with scheduled frequency | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.5            | Ensure No Expired Subscription Licenses                                                                                          | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.6            | Ensure Site-to-Site IPSec VPN is not configured with "Aggressive Mode"                                                           | <input type="checkbox"/> | <input type="checkbox"/> |
| 3.7            | Ensure Logging is enabled on firewall rules and configured to send logs to the external syslog server                            | <input type="checkbox"/> | <input type="checkbox"/> |

| Recommendation |                                                                                                                                                    | Set Correctly            |                          |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
|                |                                                                                                                                                    | Yes                      | No                       |
| 4.1            | Ensure 'Sophos X-Ops threat feeds (Advanced threat protection)' is set to 'Enabled' and Policy is set to 'Log and drop'                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.2            | Ensure Zero-day protection is enabled at the firewall rule for web protection and does not exclude any file type from zero-day protection analysis | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.3            | Ensure Zero-day protection is enabled for Email Protection and set to MTA mode                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.4            | Ensure Synchronized Security Heartbeat is enforced on Firewall Rules                                                                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.5            | Ensure MDR Threat Feeds is enabled                                                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.6            | Ensure Third-party Threat Feeds is enabled                                                                                                         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.1            | Ensure Web Policy is configured to block inappropriate URLs, Malware and content scanning is configured correctly.                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.4            | Ensure Intrusion Prevention(IPS) policy is configured on active firewall rules                                                                     | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.5            | Ensure Web Application Firewall (WAF) is configured with appropriate protection policies in all the WAF rules in use                               | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.8            | Ensure Firewall Rules with SMB, Netbios, RDP and other unencrypted protocols should not be directly accessible from WAN Zone                       | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.9            | Ensure Wireless Protection is configured with secure configuration                                                                                 | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.10           | Ensure No Firewall Rules with source 'ANY', service 'ANY' and destination 'ANY' from 'WAN' Zone                                                    | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: CIS Controls v8 Unmapped Recommendations

| Recommendation |                                                         | Set Correctly            |                          |
|----------------|---------------------------------------------------------|--------------------------|--------------------------|
|                |                                                         | Yes                      | No                       |
| 1.1.8          | Ensure MFA for Web console access and remote access VPN | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.9          | Ensure MFA for default admin                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 1.1.10         | Set Hostname                                            | <input type="checkbox"/> | <input type="checkbox"/> |
| 4.7            | Ensure NDR Essentials is enabled and configured         | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.11           | Ensure a Optimal Firewall health check score            | <input type="checkbox"/> | <input type="checkbox"/> |
| 5.12           | Ensure Sophos DNS protection is configured              | <input type="checkbox"/> | <input type="checkbox"/> |

# Appendix: Change History

| Date | Version | Changes for this version |
|------|---------|--------------------------|
|      |         |                          |