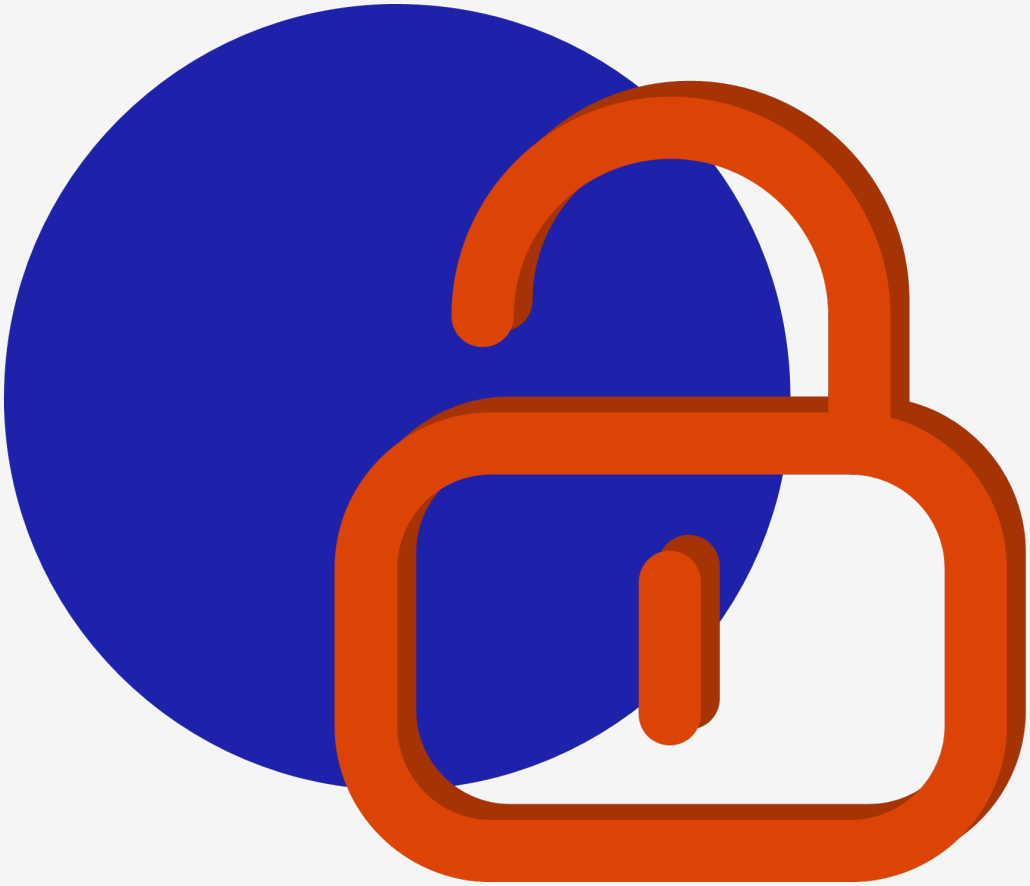
++

ZTNA AWS Environment and Sophos Firewall Security Review: Letter of Attestation

Sophos

26 January 2024



MWR CYBERSEC

Document Control

Date	Change By	Change	Issue
2023–10–12	Christopher Panayi	Document created	0.1
2023–10–12	Colman Mbuya	Document amended	0.1
2023–10–12	Muhummud Deedat	Document amended	0.1
2023–12–21	Tinus Green	Document QA	0.2
2023–12–21	Roy Fisher	Document QA	0.2
2023–12–21	Christopher Panayi	Document published	1.0
2024–01–26	Christopher Panayi	Document amended	1.5
2024–01–26	Christopher Panayi	Document published	2.0

Document Distribution

Date	Name	Company
2024–01–26	Luke Groves	Sophos

Contents

1. Overview

MWR CyberSec (MWR) conducted a security assessment of the Sophos Firewall software and the cloud web services it consumes to support its core functionality, as well as its integration with Sophos' ZTNA service. The full assessment was conducted from the 11th of September to the 12th of October 2023.

The assessment aimed to identify vulnerabilities in critical components of the Firewall and in the external integrations with Sophos' environment that could be used to exploit (or meaningfully contribute to the exploitation of) Sophos or their clients.

2. Approach

The assessment focused on the following components:

- The web portals exposed by the Sophos Firewall.
- The APIs consumed by the firewall for cloud services and those used to facilitate the device's Zero Trust Network Access (ZTNA) integration.
- The software used by the firewall during operation.
- The configuration of the relevant cloud environment in use to support the ZTNA service.

Testing of the firewall software followed a white-box approach in the time allocated, with the testing team having access to architecture details, source code and the development team, where necessary. The review focused on identifying and understanding the functions of the external services of the firewall, which were considered the main attack surface of concern. Included was web application testing of the firewall's web portals. This testing was combined with a review of the IPC mechanisms used by the firewall and instrumented fuzz-testing of selected firewall software.

Testing also aimed to prioritise newer features and functionality, where appropriate. One of the larger components that fell into this category was the ZTNA services that were assessed. This comprised of web service testing and a review of the configuration of associated cloud services.

3. Results

Overall, the Sophos Firewall - as well as its supporting web services and the ZTNA AWS environment - had a good security posture, as no vulnerabilities were found that could allow an attacker to fully compromise either the firewall software or the AWS environment. In total, 23 vulnerabilities were found; the table below shows a count breakdown of these vulnerabilities per component and risk rating.

Assessment	HIGH	MEDIUM	LOW	INFORMATIONAL
Sophos Firewall Web Application Assessment	0	1	3	2
Sophos Central and ZTNA Web Services Security Assessment	0	0	2	2
ZTNA AWS Environment Configuration Review	0	3	5	3
Sophos Firewall Security Review	0	1	1	0
Total	0	5	11	7

The majority of the vulnerabilities found were due to missing hardening controls and defence-in-depth measures that could be applied to further limit the risk of an attacker compromising the firewall software or AWS environment under specific conditions.

The following risk profiles were used as guidelines to classify the vulnerabilities:

HIGH	A vulnerability will be assessed as representing a high risk if it holds the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability which could allow an attacker to gain unauthorised access to a system or to sensitive data would be assessed as a high risk. Such issues could ultimately result in the defacement of a web site, the alteration of data held within a database or the capture of sensitive information such as account credentials or credit card information.
MEDIUM	A vulnerability will be assessed to represent a medium risk if it holds, when combined with other factors or issues, the potential for an attacker to control, alter or delete Sophos's electronic assets. For example, a vulnerability that could enable unauthorised access to be gained if a specific condition was met, or an unexpected change in configuration was to occur, would be rated as a medium risk.
LOW	A vulnerability will be assessed to represent a low risk if the likelihood or impact of exploitation is extremely low. For example, this could be an HTTPS configuration that allows weak ciphers or outdated protocols, or a CAPTCHA that can be solved programmatically.
INFORMATIONAL	A vulnerability will be assigned the informational classification when it cannot be exploited directly but is not in line with security best practice. Such a vulnerability could provide information that would facilitate research into an attack against the target system. For example, disclosure of the server type in an HTTP response.

APPENDIX I – Disclaimer and Non-Disclosure Agreement

Non-Disclosure Statement

This report is the sole property of Sophos. All information obtained during the testing process is deemed privileged information and not for public dissemination. MWR CyberSec pledges its commitment that this information will remain strictly confidential. It will not be discussed or disclosed to any third party without the express written consent of Sophos. MWR CyberSec strives to maintain the highest level of ethical standards in its business practice.

Non-Disclosure Agreement

MWR CyberSec and Sophos have signed an NDA.

Disclaimer

This report is not meant as an exhaustive analysis of the level of security now present on the tested hosts, and the data shown here should not be used alone to judge security of any computer system. Some scans were performed automatically and may not reveal all the possible security holes present in the system. In accordance with the terms and conditions of the original quotation, in no event shall MWR CyberSec or its employees or representatives be liable for any damages whatsoever including direct, indirect, incidental, consequential loss or other damages.

APPENDIX II – Project Team

Assessment Team

Lead Consultant	Christopher Panayi
Additional Consultants	Colman Mbuya Muhummud Deedat

Quality Assurance

QA Consultants	Tinus Green Roy Fisher

Project Management

Delivery Manager	Catherine de Wet
Account Director	Gaylen Postiglioni

MWR CYBERSEC