CRO CYBER RATINGS.ORG

DATA SHEET

SSE Spot Check

January 22, 2024

v1.0

© 2024 CyberRatings.org. All rights reserved.

Overview

Security Service Edge (SSE)

Security Service Edge (SSE) solutions leverage the cloud's scalability, flexibility, and operational benefits to deliver security – Access Control, Authentication and Identity, Data Loss Prevention (DLP), DNS Protection, Encryption (TLS/SSL), Exploit Detection and Prevention, Malware and Phishing Protection (including via Browser Isolation), Cloud Access / Application Control (CASB), and the ability to implement Zero Trust Network Access (ZTNA).

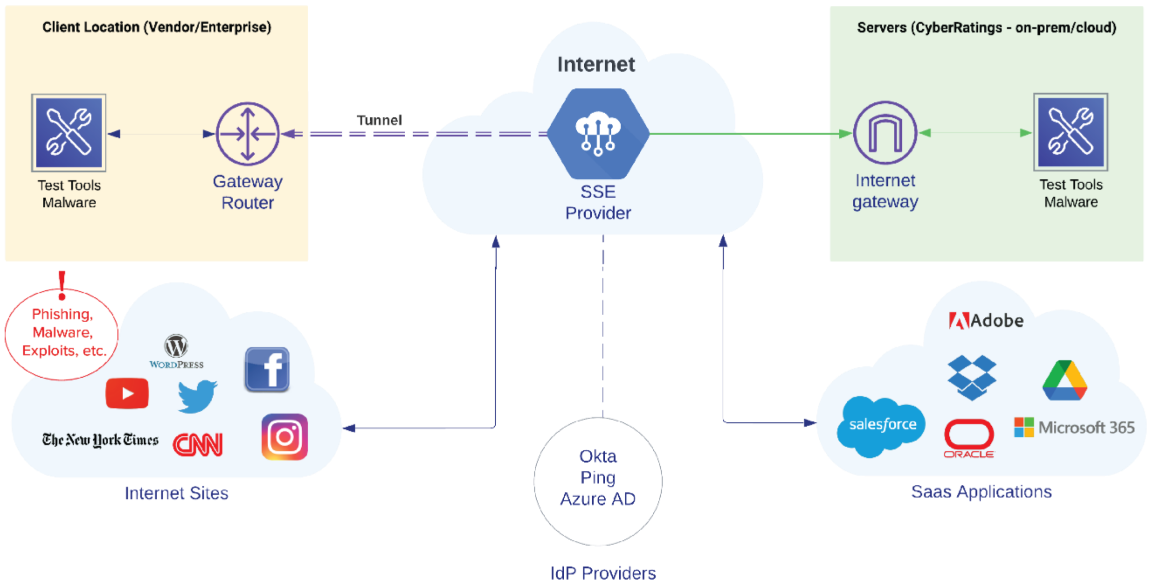
"Spot Check" is designed to answer the question, "***How do you know?***" by assessing the ability of a Security Service Edge (SSE) to block exploits and malware downloads, while remaining resistant to evasions.

What Will Be Checked?

The scope of the spot check includes:

- Basic TLS/SSL Functionality
- Protection vs. Exploits
- Protection vs Malware Download
- Resistance to Evasions
- False Positive Rate

Secure Service Edge (SSE) - Malware Downloads
SSE Test Topology



How Does It Work?

Spot Check is a virtual user that inherits the SSE policy being used by an organization. If the organization has multiple policies based on roles (e.g., Sales, Marketing, Engineering, Accounting, Executives) we recommend doing a spot check for each user type.

© 2024 CyberRatings.org. All rights reserved.

Spot Check Parameters

Cipher Suite Support

To provide visibility into potential threats that are encrypted using TLS/SSL, the SSE is expected to support a wide range of commonly used cipher suites. Cipher suites are selected based on the published current frequency of use[1] and security status[2].

Table 1 – Selected Cipher Suites[3]

Version	(Value)	Cipher Suites	Prevalence
TLS 1.3	(0x13, 0x02)	TLS_AES_256_GCM_SHA3	66.51%
TLS 1.2	(0xC0, 0x30)	TLS_ECDHE_RSA_WITH_A	11.85%
TLS 1.2	(0xC0, 0x2F)	TLS_ECDHE_RSA_WITH_A	9.26%
TLS 1.3	(0x13, 0x01)	TLS_AES_128_GCM_SHA2	8.07%
TLS 1.2	(0xCC, 0xA8)	TLS_ECDHE_RSA_WITH_C	1.72%
TLS 1.2	(0xC0, 0x28)	TLS_ECDHE_RSA_WITH_A	0.68%
TLS 1.3	(0x13, 0x03)	TLS_CHACHA20_POLY130	0.55%
TLS 1.2	(0xC0, 0x2C)	TLS_ECDHE_ECDSA_WITH	0.42%
TLS 1.2	(0xCC, 0xA9)	TLS_ECDHE_ECDSA_WITH	0.27%
TLS 1.2	(0xC0, 0x2B)	TLS_ECDHE_ECDSA_WITH	0.20%

False Positives

False positives are legitimate, non-malicious traffic that the SSE perceives as malicious and blocks. The ability to correctly identify and allow legitimate traffic while maintaining protection against attacks is a key to effective protection. False positive tests examine the ability of the SSE to block attacks while permitting legitimate traffic.

Ongoing check – legitimate traffic, documents, and files

Since SSE is a cloud offering that, in some cases, utilizes machine learning to modify/tune settings in real-time, testing for false positives requires legitimate traffic and documents to be included when testing the SSE offering's ability to block attacks. CyberRatings will introduce legitimate traffic, documents, and files into the malware download and exploit protection tests. Testing may include but is not limited to: HTML, .exe, .jar, .xlsm, .css, .pdf, .ppt, .pptx, .doc, .docx, .zip, 7zip, gzip, .DLL, .js, .xls, .xlsx, .chm, .rar, .Ink, .cur, .tar, .xrc.

Exploit Protection

An exploit is an attack that takes advantage of a vulnerability in a protocol, product, operating system, or application. CyberRatings verifies that the Security Service Edge can detect and block exploits while remaining resistant to false positives by attempting to send exploits through the SSE and verifying that the malicious traffic is blocked.

[1] Published international daily cipher suite usage can be found at https://crawler.ninja/files/ciphers.txt

[2] A list of cipher suites and associated attributes including security ratings can be found at https://ciphersuite.info/cs/

[3] Cipher suite descriptions and associated value codes for testing are from https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml.

The CyberRatings exploit repository contains exploits covering a wide range of protocols and applications. Exploit sets are selected based on CVSS score (how widely used is an application + what can an attacker do?), use case, and customer relevance.

Malware Protection

Malware is malicious software that is intentionally designed to cause harm to targeted computers. CyberRatings verifies that the Security Service Edge can detect and block malware while remaining resistant to false positives by attempting to send malware through the SSE and verifying that the malicious file is blocked.

CyberRatings maintains relationships with other independent security researchers, professional networks, and security companies from which we obtain and catalog malware. Malware sets are selected based on platform, freshness, impact, and customer relevance.

Resistance to Evasions

Threat actors use evasion techniques to disguise and modify attacks at the point of delivery to avoid detection by security products. It is imperative that a firewall correctly handles evasions since just one successful evasion technique can enable an attacker to compromise systems undetected.

CyberRatings first verifies that the firewall detects and blocks a collection of baseline exploits and malware. Next, CyberRatings applies evasion techniques to the baseline exploits and malware and validates the execution of the exploit's payload or the malware's delivery. Wherever possible, the firewall is expected to successfully normalize the evaded traffic to provide an accurate alert relating to the original attack, rather than alerting purely on anomalous traffic detected because of the evasion technique itself.

Supported Systems

SSE Providers

Spot Check supports all popular SSE providers via IPSEC or GRE tunnels.

SAML Authentication

Spot Check supports all popular SAML providers (Microsoft AD, Okta, Ping, etc.).

Contact Information

CyberRatings.org
2303 Ranch Road 620 South
Suite 160, #501
Austin, TX 78734
info@cyberratings.org
www.cyberratings.org

© 2024 CyberRatings. All rights reserved. No part of this publication may be reproduced, copied/scanned, stored on a retrieval system, emailed, or otherwise disseminated or transmitted without the express written consent of CyberRatings ("us" or "we").

Please read the disclaimer in this box because it contains important information that binds you. If you do not agree to these conditions, you should not read the rest of this report but should instead return the report immediately to us. "You" or "your" means the person who accesses this report and any entity on whose behalf he/she has obtained this report.

1. The information in this report is subject to change by us without notice, and we disclaim any obligation to update it.

2. The information in this report is believed by us to be accurate and reliable at the time of publication but is not guaranteed. All use of and reliance on this report are at your sole risk. We are not liable or responsible for any damages, losses, or expenses of any nature whatsoever arising from any error or omission in this report.

3. NO WARRANTIES, EXPRESS OR IMPLIED ARE GIVEN BY US. ALL IMPLIED WARRANTIES, INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT, ARE HEREBY DISCLAIMED AND EXCLUDED BY US. IN NO EVENT SHALL WE BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, INCIDENTAL, PUNITIVE, EXEMPLARY, OR INDIRECT DAMAGES, OR FOR ANY LOSS OF PROFIT, REVENUE, DATA, COMPUTER PROGRAMS, OR OTHER ASSETS, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

4. This report does not constitute an endorsement, recommendation, or guarantee of any of the products (hardware or software) tested or the hardware and/or software used in testing the products. The testing does not guarantee that there are no errors or defects in the products or that the products will meet your expectations, requirements, needs, or specifications, or that they will operate without interruption.

5. This report does not imply any endorsement, sponsorship, affiliation, or verification by or with any organizations mentioned in this report.

6. All trademarks, service marks, and trade names used in this report are the trademarks, service marks, and trade names of their respective owners.

© 2024 CyberRatings.org. All rights reserved.