What does "Secure by Default" Mean for Security Service Edge Solutions?

Security Service Edge (SSE) Mini-Test Results

The security level of SSE products in their default configuration varies significantly. While many enterprise customers expect these products to reduce operational complexity by being plug-and-play, the reality is that the default security achieved with such a deployment may not be sufficient to meet their specific needs.

Key Findings

- The level of security offered by default varies greatly across SSE vendors. Three out of seven SSE vendors tested offered no security by default.
- In some cases, minor changes from a vendor's supplied default configuration dramatically improved the security posture of an SSE solution. We observed improvements in malware blocking from 0% to >90% on average.
- SSE customers should not assume any level of security by default without verification.
- SSE customers should understand where the SSE they use stands by default, and whether that default offers the required level of security for their environment.
- SSE customers should be aware of the potential default options and their implications during any guided setup offered, which may not provide the required level of security. This can be a risk when leveraging non-technical staff for initial setup and configuration.

Background

SSE solutions are a subset of Secure Access Service Edge (SASE) that focus primarily on security services delivered through the cloud. SSE encompasses critical security functions such as Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), and Zero Trust Network Access (ZTNA), which work together to protect users, devices, and applications across distributed networks. By shifting these security functions to the cloud, SSE solutions improve flexibility and scalability, enabling enterprises to enforce security policies regardless of user location or device. SSE is particularly beneficial for organizations with a remote or hybrid workforce, as it provides consistent protection against threats, controls access to cloud services and ensures data security without relying on traditional network boundaries.

Introducing "Mini-Tests"

The goal of this first iteration of CyberRatings' SSE Mini-Test was to derive some empirical data to help answer the question: "Are SSE products secure by default?"

This mini test intentionally did not constitute a comprehensive security evaluation of the full capabilities or overall effectiveness of the vendor platforms. Instead, it focused on a data driven "quick look" at the default posture as delivered by vendors, and with minimal to no additional security configuration of the SSE. The idea was to test the initial basic functional working state. The results of this particular mini test should not be construed as representative of the overall effectiveness or capabilities of the SSE platforms tested.

Why We Tested

There is a notable shift in the industry towards "secure by default" approaches to developing and deploying cybersecurity products. Research indicates that most customers expect cybersecurity vendors to ship with a high level of protection enabled *by default*. CISA's publication states the following:

"Secure-by-Default" means products are resilient against prevalent exploitation techniques out of the box without additional charge. These products protect against the most prevalent threats and vulnerabilities without end-users having to take additional steps to secure them. Secure-by-Default products are designed to make customers acutely aware that when they deviate from safe defaults, they are increasing the likelihood of compromise unless they implement additional compensating controls.

A secure configuration should be the default baseline. Secure-by-Default products automatically enable the most important security controls needed to protect enterprises from malicious cyber actors, as well as provide the ability to use and further configure security controls at no additional cost.

Test Methodology

For each of the vendors tested, we performed the following tests using Windows 11 clients configured with the vendor's SSE client software:

- Test 1: Download ~1,000 benign samples over HTTP designed to be susceptible to being classified as malware despite being innocuous (e.g. the solution's propensity for triggering false positives).
- Test 2: Download ~3,000 active malware samples, current to within 30 days of the test, over HTTP (e.g. the SSE's ability to detect and block basic malware downloads). There were no evasions applied.

Results & Observations

In this first comparison, three out of seven vendors had 0% malware downloads blocked using their default configuration. Four vendors achieved malware download blocking scores from 89.90% to 96.74%. For products whose default configurations offered 0% protection we made minor configuration changes to determine how much the protection could improve. With those changes, we were able to achieve over 90% block rate on average. For products that offered effective defaults, no further adjustments were made.

SSE Mini-Test Results

SSE Vendor	Malware Downloads Blocked (Higher is Better)	False Positives (Lower is Better)	Sandboxing Included in License / Enabled
Check Point (default)	0.00%	0.00%	No / No
Check Point (non-default)	89.96%	0.00%	No / No
Cisco (default)	0.00%	0.00%	Yes / No
Cisco (non-default)	100.00%	0.13%	Yes / Yes
Cloudflare (default)	95.27%	5.70%	Unknown
Fortinet (default)	89.90%	0.00%	No / No
Skyhigh (default)	91.53%	0.66%	Unknown
Versa Networks (default)	0.00%	0.00%	No / No
Versa Networks (non-default)	83.86%	0.93%	No / No
Zscaler (default)	96.74%	0.00%	Yes / Yes

Observations

While some SSEs offer moderate malware protection by default, others do not. End-users should verify the security level their organizations require and assess whether the vendor's default configuration meets their needs. If it does not, it is advisable to implement the vendor's recommended best practices and configurations for an optimized solution. It should not be assumed that any vendor solution will be secure by default.

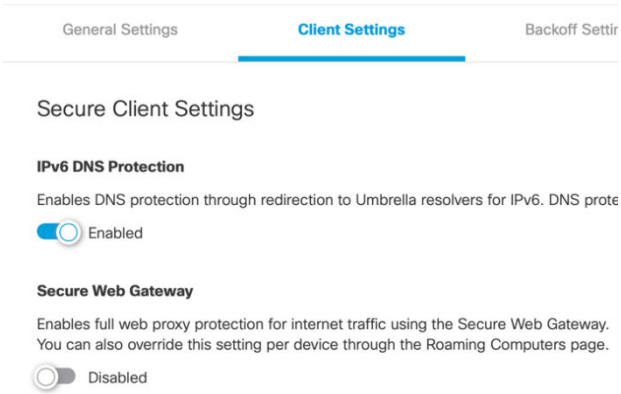
Additionally, our testing found that sandboxing technology significantly enhanced malware detection. Due to variations in product packaging and licensing across vendors, sandboxing capabilities may or may not be included in their offerings. SSE solutions that included sandboxing as part of the licensed features we acquired were generally more effective at detecting malware. As a result, CyberRatings considers sandboxing a critical security feature that end users should prioritize when selecting products and licensing.

In this mini test, not all vendor licenses included sandboxing technology. For future mini tests, configurations both with and without sandbox technology will be tested to ensure that we provide the best possible coverage as these solutions evolve. This underlines why the results of this mini-test should not be seen as a comprehensive assessment of the overall security effectiveness of SSE platforms, as it primarily focused on the security offered in the simplest "default" configuration for each vendor.

The configuration required to achieve an acceptable level of protection can vary significantly between vendors. For instance, the Cisco Umbrella, Versa, and Checkpoint solutions, do not enable inspection by default.

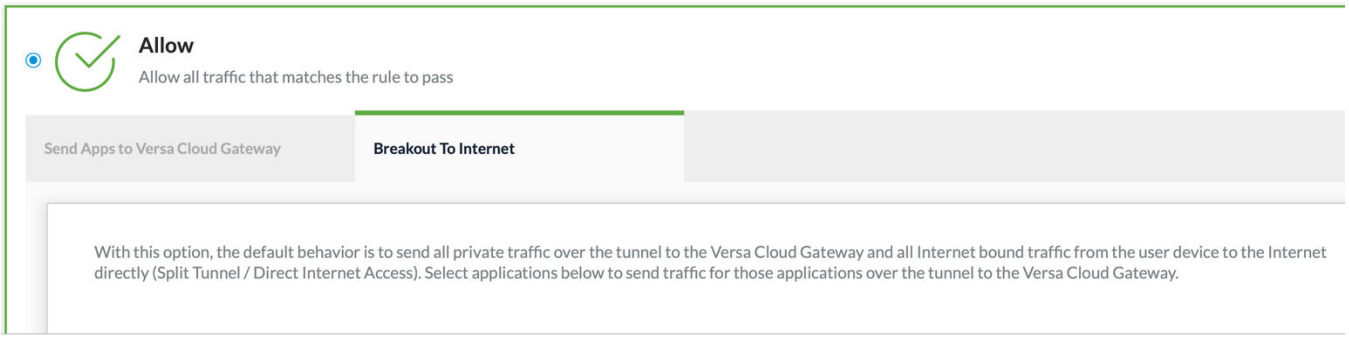
Cisco

By enabling the Secure Web Gateway setting, a setting tucked away in a tab of a settings page, the Cisco Umbrella solution will force all traffic to be inspected by the Secure Web Gateway (SWG) inspection engine. With this simple change, the Cisco solution went from blocking 0% of our malware sample set to blocking 100%. This represents a dramatic improvement with a simple configuration change that should have been enabled by default.



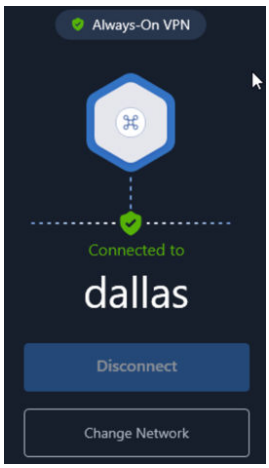
Versa Networks

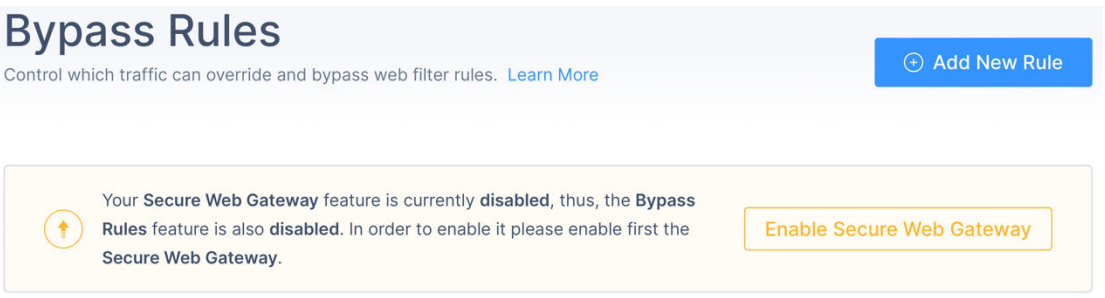
When going through the initial setup for Versa's Secure Client Access rules, the guided setup UI defaults to the insecure default of sending all Internet bound traffic directly to the Internet, bypassing the solution's inspection engine. Deviating from the guided default and clicking "Send Apps to Versa Cloud Gateway" drastically improved the solution's malware block rate from 0% to 84%.



Check Point

After creating a network and deploying a gateway in the admin panel, deployed clients are presented with a positive green status that their machine is connected. However, at this point web filtering is not enabled. After going back into the admin panel and explicitly enabling the Secure Web Gateway (web filtering) feature, the malware block rate improved from 0% to 90%.





Summary & Conclusion

The findings from CyberRatings' inaugural SSE Mini-Test reveal significant variability in the security effectiveness of SSE products in their default configurations. While the industry works to adopt a "secure by default" stance, our tests indicate that current definitions of the default security level may not always meet the specific needs of enterprise customers. It is essential for organizations to critically assess whether a vendor's out-of-the-box configuration offers sufficient protection or if further customization or licensing is required.

Our testing showed that a simple configuration change, such as enabling a security inspection engine that is not enabled by default, can drastically improve protection, highlighting the importance of understanding and optimizing security settings.

Organizations must not assume that any SSE product is secure by default. Instead, they should validate the security measures needed for their environment and leverage vendor-recommended best practices to achieve an optimized, secure configuration. The insights from this mini test underscore the necessity for continuous evaluation and adjustment of security settings to stay ahead of emerging threats and ensure robust protection.

As a reminder, this mini test was not designed or intended to measure the overall potential effectiveness of SSE platforms. This mini test is intended to provide insight into the default security posture across SSE platforms using a small subset of our malware samples (using ~3,000 samples vs the 100,000+ samples in our more all-inclusive tests). CyberRatings' full testing programs and resulting reports employ much more.

SPECIAL THANKS

We would like to thank Keysight for providing technology and support for our variety of testing programs.

AUTHORS

Ian Foo, Thomas Skybakmoen, Vikram Phatak, Edsel Valle, Tim Otto

CONTACT INFORMATION

CyberRatings.org

515 South Capital of Texas Highway

Suite 225

Austin, TX 78746

info@cyberratings.org

www.cyberratings.org