MPLIFY

Testing Guide

SSE Certification Blueprint

July 2025 | Version 1.0

Contents

Figures

Introduction

This document specifies the SSE Certification test categories, descriptions, requirement IDs, test cases and requirements (TC & R) references, and scoring used as part of the SASE Certification Program – Phase 1, based on:

- MEF 138 *Security Functions for IP Services*
- MEF 162 *Draft R3 Security Service Edge Certification Test Cases and Requirements*

Scope

SSE Certification includes the following test categories:

- TLS/SSL Functionality
- Exploit Protection
- Malware Protection
- Evasion Protection
- Performance

Out of scope:

Management and orchestration of SSE Services, LSO APIs, IPsec transport protocol, generation of Security Event Notifications and how state is tracked by security functions.

SSE Certification Framework

The SSE Certification Framework is composed of the following eight parts:

- Test Cases & Requirements
- Topology
- TLS/SSL Functionality Scoring
- Exploit Protection Scoring
- Malware Protection Scoring
- Evasion Protection Scoring
- Scoring Methodology
- Scoring Example

1. Test Cases & Requirements

Category: TLS/SSL Functionality			
Description	**SSE Requirement ID**	**TC & R Reference**	**Scoring Impact**
For each Security Function, the Service Provider MUST maintain a list of criteria entries in the Block List.	MEF 138 R1	MEF 162 Draft R3 9.1.2	Yes
For each Security Function, the Service Provider MUST maintain a list of criteria entries in the Allow List.	MEF 138 R7	MEF 162 Draft R3 9.2	Yes
Based on agreement with the Subscriber, the Service Provider MUST maintain a list of criteria entries in the Supported List for each Security Function that uses a Supported List.	MEF 138 R11	MEF 162 Draft R3 9.2	Yes
Based on agreement with the Subscriber, the Service Provider MUST maintain a list of criteria entries in the Unsupported List for each Security Function that uses an Unsupported List.	MEF 138 R12	MEF 162 Draft R3 9.2	Yes
The Service Provider MUST ensure that a criteria entry on the Supported List for a given Security Function cannot also appear on the Unsupported List for that Security Function.	MEF 138 R13	MEF 162 Draft R3 9.2	Yes
When the Middlebox Security Function supports TLS, each Middlebox Security Function List MUST contain the following criteria entry parameters for TLS: Type of encryption protocol: *TLS* Protocol Version, e.g., *1.1, 1.2, 1.3*… List of Cipher Suites for a given TLS protocol version (any can be used to indicate that any cipher suite for a given TLS protocol version is on the list)	MEF 138 R37	MEF 162 Draft R3 9.1.1	Yes
The Middlebox Security Function MUST support at least one of the following secure transport protocols: Transport Layer Security (TLS) IPsec	MEF 138 R45	MEF 162 Draft R3 9.1.2	Yes
When TLS is supported, the Middlebox Security Function MUST meet the mandatory requirements of TLS 1.2, per RFC 5246.	MEF 138 R48	MEF 162 Draft r3 9.2	Yes
When TLS is supported, the Middlebox Security Function MUST meet the mandatory requirements of Section 9.3 of RFC 8446 (Protocol Invariants).	MEF 138 R49	MEF 162 Draft R3 9.2	Yes

Category: Malware Protection			
Description	**SSE Requirement ID**	**TC & R Reference**	**Scoring Impact**
The test MUST verify that Malware is blocked while legitimate traffic is passed. Note: Approximately 6000 malware samples are used in testing.	-	MEF 162 Draft R3 12.3	Yes
When a Malware Detection and Removal Security Function Policy is included in a Security Policy for a given Service Flow, the Service Provider MUST meet the mandatory requirements specified in Section 6.1 of MEF 138 relating to the Malware Detection and Removal Block List, the Malware Detection and Removal Allow List and the Malware Detection and Removal Quarantine List.	MEF 138 R83	MEF 162 Draft R3 12.3	Yes
When a Malware Detection and Removal Security Function is included in a Service Policy for a given Service Flow, the Service Provider MUST support both of the following actions for a subset of the Service Flow that does not match a criteria entry on any of the Malware Detection and Removal Filtering lists: Block the subset of the Service Flow Allow the subset of the Service Flow	MEF 138 R85	MEF 162 Draft R3 12.3	Yes
When a Malware Detection and Removal Security Function is included in a Service Policy for a given Service Flow, the Malware Detection and Removal Security Function MUST perform one of the following actions for each subset of the Service Flow that does not match a criteria entry on any of the Malware Detection and Removal lists: Block the subset of the Service Flow Allow the subset of the Service Flow	MEF 138 R86	MEF 162 Draft R3 12.3	Yes
When a Malware Detection and Removal Security Function is included in a Service Policy for a given Service Flow, and when a subset of the Service Flow is determined to either have Malware or look suspicious that it may have Malware, the Malware Detection and Removal Security Function MUST perform one of the following actions, based on agreement between the Service Provider and the Subscriber: Block the Service Flow Block the subset of the Service Flow containing the Malware and Allow the remainder of the Service Flow Quarantine the Service Flow Quarantine the subset of the Service Flow containing the Malware and Allow the remainder of the Service Flow Remove Malware from the Service Flow and Allow the Service Flow	MEF 138 R87	MEF 162 Draft R3 12.3	Yes

Category: Exploit Protection			
Description	**SSE Requirement ID**	**TC & R Reference**	**Scoring Impact**
The test MUST verify that exploits are blocked while legitimate traffic is passed. *Note: Approximately 200 exploits are used in testing.*	-	MEF 162 Draft R3 12.2	Yes

Category: Evasion Protection			
Description	**SSE Requirement ID**	**TC & R Reference**	**Scoring Impact**
The test MUST verify that HTTP evasions are detected.	-	MEF 162 Draft R3 13.1	Yes
The test MUST verify that HTML Obfuscations are detected.	-	MEF 162 Draft R3 13.2	Yes
The test MUST verify that Malware within Packers are detected.	-	MEF 162 Draft R3 13.3	Yes
The test MUST verify that Malware within Compressors are detected.	-	MEF 162 Draft R3 13.4	Yes
When a combination of evasion methods is used in testing, the test MUST verify all evasions are detected.	-	MEF 162 Draft R3 13.5	Yes

Category: Performance			
Description	**SSE Requirement ID**	**TC & R Reference**	**Scoring Impact**
This test determines the maximum throughput across the SSE solution.	-	Industry Best Practice 1	No

2. Topology

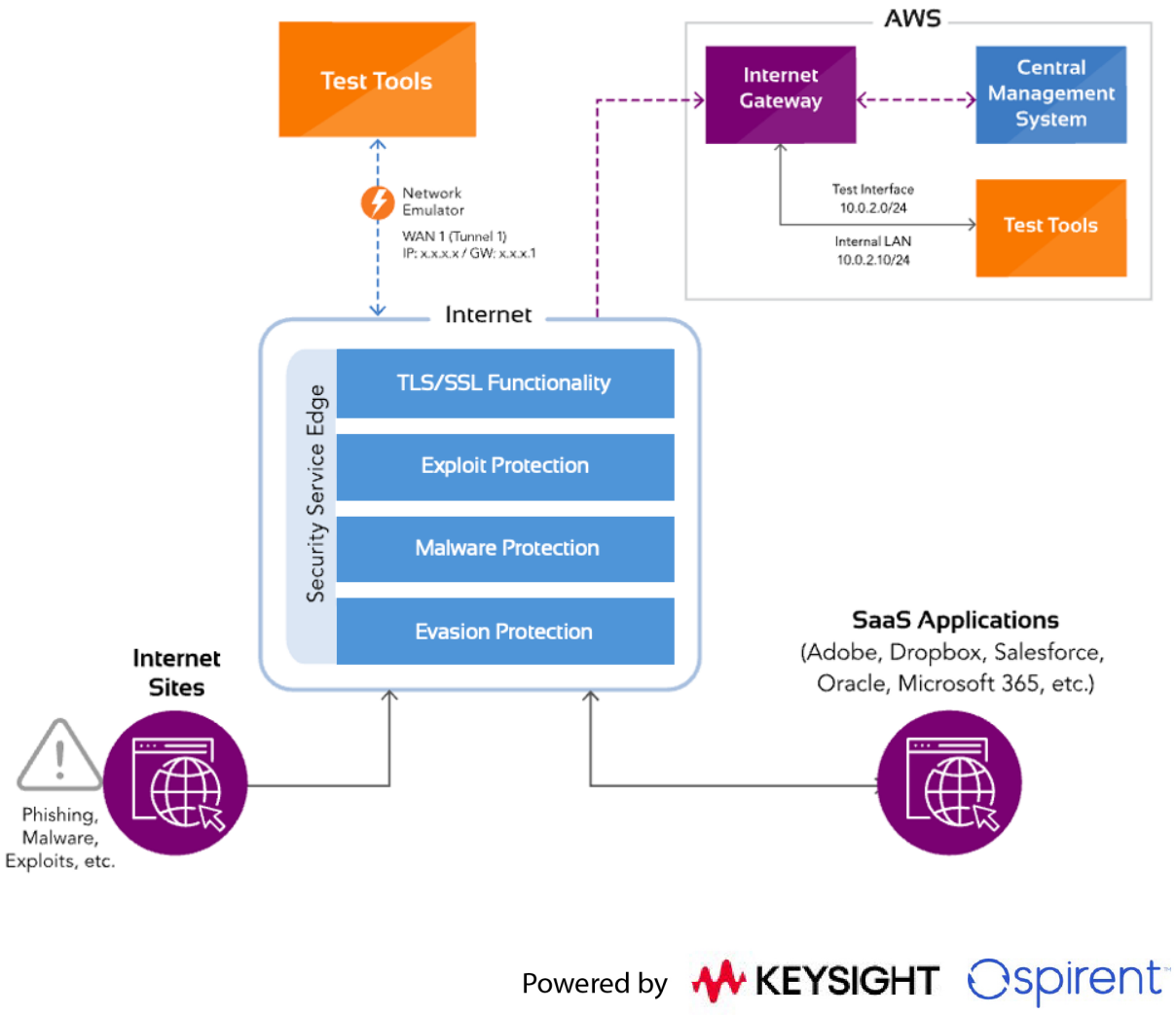

Figure 1 – SSE Certification Topology

3. TLS/SSL Functionality Scoring

The TLS/SSL Functionality score is determined by deducting the prevalence percentage for any missed TLS/SSL cipher suites from 100%.

TLS/SSL Prevalence		
Version	**Prevalence**	**Cipher Suites**
TLS 1.3	66.51%	TLS_AES_256_GCM_SHA384 (0x13, 0x02)
TLS 1.2	11.85%	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)
TLS 1.2	9.26%	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)
TLS 1.3	8.07%	TLS_AES_128_GCM_SHA256 (0x13, 0x01)
TLS 1.2	1.72%	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA8)
TLS 1.2	0.68%	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28)
TLS 1.3	0.55%	TLS_CHACHA20_POLY1305_SHA256 (0x13, 0x03)
TLS 1.2	0.42%	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)
TLS 1.2	0.27%	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA9)
TLS 1.2	0.20%	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B)

4. Exploit Protection Scoring

The Exploit Protection Score is a direct percentage of the Exploits detected and blocked. The Test sends approximately 200 exploits to be detected.

5. Malware Protection Scoring

The Malware Protection Score is a direct percentage of the malware samples detected and blocked. The Test sends approximately 6000 malware samples to be detected.

6. Evasion Protection Scoring

The Evasion Protection Scoring is calculated by averaging the Malware Evasion Resistance Score and the Exploit Evasion Resistance Score.

6.1. Malware Evasion Resistance

The Malware Evasion Resistance Score is calculated by determining the penalty associated with missing a malware-based evasion as describes in the table below and subtracting the cumulative penalty value from 100%.

Malware-based Evasion Resistance Penalties		
Evasion Technique Category	**Penalty**	**Max Penalty**
Packers	50%	100%
Compressors	50%	
Compressors and HTTP Compression	50%	
Compressors and HTTP Headers	50%	
Compressors and HTTP Chunked Encoding	50%	
Compressors, HTTP Compression, and HTTP Chunked Encoding	50%	
HTTP Compression	20%	60%
HTTP Headers	20%	
HTTP Chunked Encoding	20%	
HTTP Compression and HTTP Chunked Encoding	20%	

6.2. Exploit Evasion Resistance

The Exploit Evasion Resistance Score is calculated by determining the penalty associated with a missed exploit-based evasions as described in the table below and subtracting the cumulative penalty value from 100%.

Exploit-based Evasion Resistance Penalties		
Evasion Technique Category	**Penalty**	**Max Penalty**
HTTP Compression	20%	60%
HTTP Compression and HTTP Chunked Encoding	20%	
HTTP Compression, HTTP Chunked Encoding and HTTP Headers	20%	
HTTP Headers	20%	
HTTP Chunked Encoding	20%	
HTTP Obfuscation	20%	
HTML	1%	10%
HTML Obfuscation	1%	
HTML and HTTP Headers	1%	
HTML and HTTP Compression	1%	
HTML and HTTP Chunked Encoding	1%	
HTTP Chunked Encoding and HTTP Headers	1%	
HTML, HTTP Compression, HTTP Chunked Encoding and HTTP Headers	1%	
HTML, HTTP Compression, and HTTP Chunked Encoding	1%	
JavaScript	1%	
JavaScript and HTTP Headers	1%	
JavaScript and HTTP Compression	1%	
JavaScript and HTTP Chunked Encoding	1%	
JavaScript, HTTP Compression and HTTP Chunked Encoding	1%	
JavaScript, HTTP Compression, HTTP Chunked Encoding and HTTP Headers	1%	
JavaScript and HTML	1%	
JavaScript, HTML and HTTP Compression	1%	
JavaScript, HTML, HTTP Compression and HTTP Chunked Encoding	1%	
JavaScript, HTML, HTTP Compression, HTTP Chunked Encoding and HTTP Headers	1%	
JavaScript, HTML and HTTP Chunked Encoding	1%	
JavaScript, HTML and HTTP Headers	1%	
Combination	1%	

7. Overall Scoring Methodology & Rating

The SSE Certification Overall Score is calculated by multiplying the TLS/SSL Functionality Score, the Exploit Protection Score, the Malware Protection Score and the Evasion Protection Score.

SSE Certification Rating Table	
Rating	**Total Credited Percentage – Overall Score**
AAA	96.88% - 100%
AA	90.00% - 96.87%
A	82.50% - 89.99%
BBB	73.75% - 82.49%
BB	67.50% - 73.74%
B	60.00% - 67.49%
CCC	52.50% - 59.99%
CC	45.00% - 52.49%
C	37.50% - 44.99%
D	00.00% - 37.49%

8. Overall Scoring Example

The following example demonstrates the calculation of an SSE Certification Overall score and final rating.

SSE Certification Scoring Example Data		
SSE Category	**Score**	**Notes**
Malware Evasion Resistance Score	100.00%	No missed Malware Evasions
Exploit Evasion Resistance Score	79.00%	Missed HTTP Headers (20%) and Combination (1%)
TLS/SSL Functionality Score	98.28%	Missed 1 cipher (0xCC, 0xA8)
Malware Protection Score	99.27%	Blocked 6,139 of 6,184 malware samples
Exploit Protection Score	100%	Blocked 205 of 205 exploits

Step 1: Calculate the Malware and Exploit Evasion Resistance Scores

- Malware Evasion Resistance Score =100%-Penalties
    - Total Malware Evasion Resistance Score = 100% - (0%) = 100%
- Exploit Evasion Resistance Score = 100% - Penalties
    - Missed HTTP headers = 20% penalty
    - Missed combination evasion = 1% penalty
    - Total exploit evasion resistance score = 100% - (20% + 1%) = 79%

Step 2: Calculate Evasion Protection Score

Average malware and exploit evasion resistance scores:

- Evasion Protection Score = (100% + 79%)/2
- Total Evasion Protection Score = 89.5%

Step 3: Calculate TLS/SSL Functionality Score

- TLS/SSL Functionality Score = (100% - Penalties)
- TLS/SSL Functionality Score = (100% – 1.72%)
- Total TLS/SSL Functionality Score = 98.28%

Step 4: Calculate Malware Protection Score

- Malware Protection Score = (Blocked/Total)
- Malware Protection Score = (6139/6184)
- Total Malware Protection Score = 99.27%

Step 5: Calculate Exploit Protection Score

- Exploit Protection Score = (Blocked/Total)
- Exploit Protection Score = (205/205)
- Total Exploit Protection Score = 100%

Step 6: Calculate SSE Certification Score

Multiply Evasion Protection Score, TLS/SSL Functionality Score, Malware Protection Score, and Exploit Protection Score:

- 89.5% x 98.28% x 99.27% x 100% = **87.32%**

Step 7: Assign SSE Certification Rating

See SSE Certification Rating Table

Final Rating: **A**

Revision History

Revision History	Date	Revision
Version 1.0	July 22, 2025	SSE Certification Blueprint Version 1.0

Testing Guide: SSE Certification Blueprint v1.0