SASE Certification: Technology Providers

Introduction

MEF 3.0 SASE (Secure Access Service Edge) Certification empowers technology providers to deliver cybersecurity services that protect enterprise customers in the constantly evolving worlds of cybercrime and cybersecurity.

The cybercrime economy is projected to reach $10.5 trillion USD annually by 2025 (source: Cybersecurity Ventures). Enterprises face increasing demands for compliance and a daunting range of cybersecurity solutions. In response to these major challenges, MEF has developed industry standards and a modular certification program underpinned by those standards.

MEF's SASE Certification enables technology providers to validate that their SASE cloud services are secure and address the persistent and increasingly malicious cyberthreats that threaten the public and private landscape.

MEF's SASE Certification tests the following functionality:

- Application performance during simulated WAN impairments.

- Scale and performance of a SASE cloud service.

- Correct classification of applications so that performance and/or security polices can be applied.

- Threat protection testing consisting of 1,000,000+ current malware samples; 2,000+ exploits that take advantage of a vulnerability in a protocol, product, operating system, or application; 10,000+ evasions that disguise and modify attacks to avoid detection by security products.

- TLS/SSL functionality to validate cryptographic suites, version functionality, etc.

- Zero Trust principles for authentication and authorization of applications, users, and devices via policies at the network level.

- Compliance with MEF standards that enable an industry-wide vocabulary, language, constructs, and service definition.
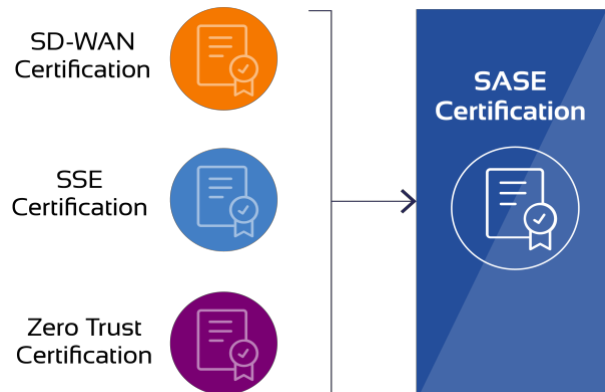
Testing Partner

MEF Accredited Test and Certification Partner (MEF-ATCP), CyberRatings.org, is a non-profit 501(c)6 entity dedicated to quantifying cyber risk and providing transparency on cybersecurity product efficacy through testing and ratings programs. CyberRatings.org provides unique security testing expertise and a proficiency spanning more than three decades of testing at the highest technical standards and building trust with vendors and enterprises worldwide. They provide tests for both remote and in-lab facilities, test suite implementations, personnel, and private testing. Their testing and certification incorporates the latest testing methodologies, including 100,000+ simultaneous VMs for emulating large environments, with automation and test systems, and additional tooling from test partners like Spirent and Keysight.

Certification Model

MEF SASE Certification is comprised of three individual certification programs:

- SD-WAN (Software-Defined Wide-Area Network)
- SSE (Security Service Edge)
- Zero Trust

A technology provider may achieve individual SD-WAN, SSE, and Zero Trust certifications, which will appear in the MEF Technologies Certification Registry, but must achieve all three certifications to become SASE certified. When all three individual certifications are achieved, a final SASE certification is issued to the technology provider. SASE certification is rendered with a scoring and rating that averages all three individual certifications, based on a rating from D (lowest) to AAA (highest).

It is possible for disaggregated SASE technology providers to describe how they integrate with other technology providers to create disaggregated SASE solutions and obtain a SASE certification. The details of this approach are more complicated and are available on a companion Q&A document available upon request.

MEF's SASE Certification program (SD-WAN, SSE, and Zero Trust) is a subscription-based Continuous Integration/Continuous Test (CI/CT) model and process that allows technology providers unlimited testing for a given type of certification and the ability to progressively improve their certification scores to deliver exceptional SD-WAN and cloud-based cybersecurity products to the market. The subscription period is 1 year for each certification from the initiation of the first tests; it should be noted that a yearly subscription must be maintained to keep any previous certifications and badges.

Implementations from a single technology provider that are running one OS (e.g., VOS) on one type of processor, are all under one certification, regardless of the number of interfaces, speed of interfaces, etc.
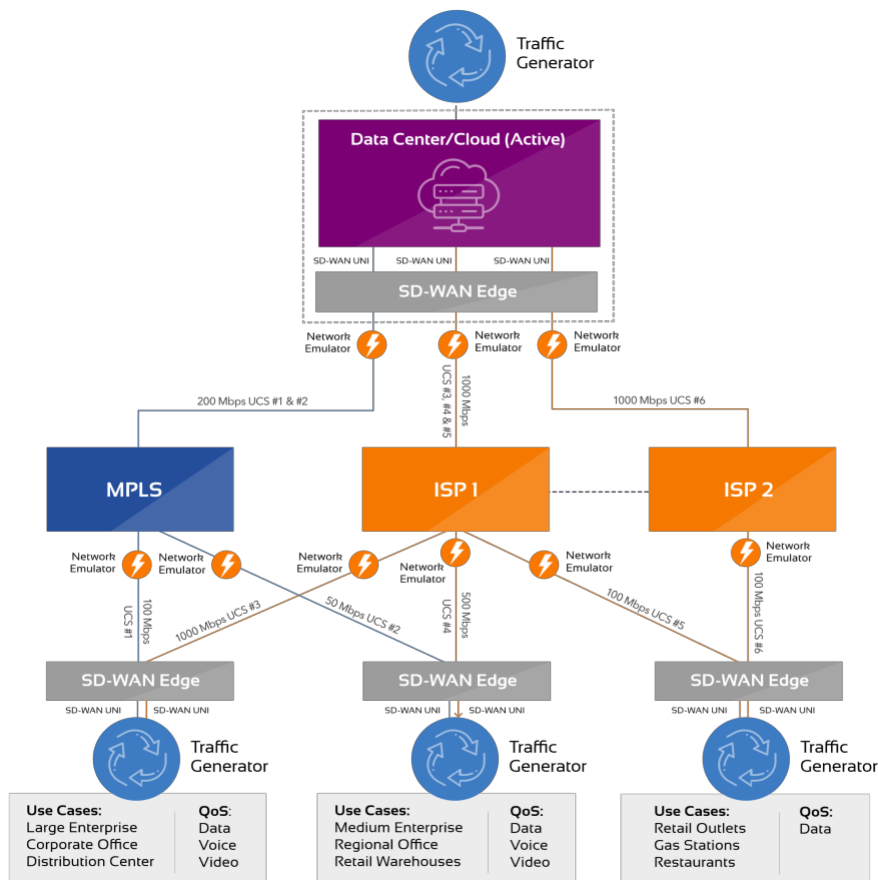
Certifications

SD-WAN Certification

SD-WAN technology is tested by creating a simulated multi-node enterprise network with each node having specific traffic and performance characteristics (e.g., datacenter, cloud, corporate office, regional office, remote office, retail outlets, etc.). Certification steps through various use cases (e.g., voice call, video call, access to files, data transfer, email, retail transaction, etc.), and access to cloud services (e.g., SharePoint, Salesforce, Dropbox, etc.). Testing is based on MEF W90.2 SD-WAN Certification Test Cases and Requirements -Phase 2.

SD-WAN policies are applied, and the SD-WAN is tested for:

- Routing and Access Control

- WAN Impairments

- Performance

- Classification Verification

- Conformance to MEF 70.1 SD-WAN Service Attributes and Service Framework
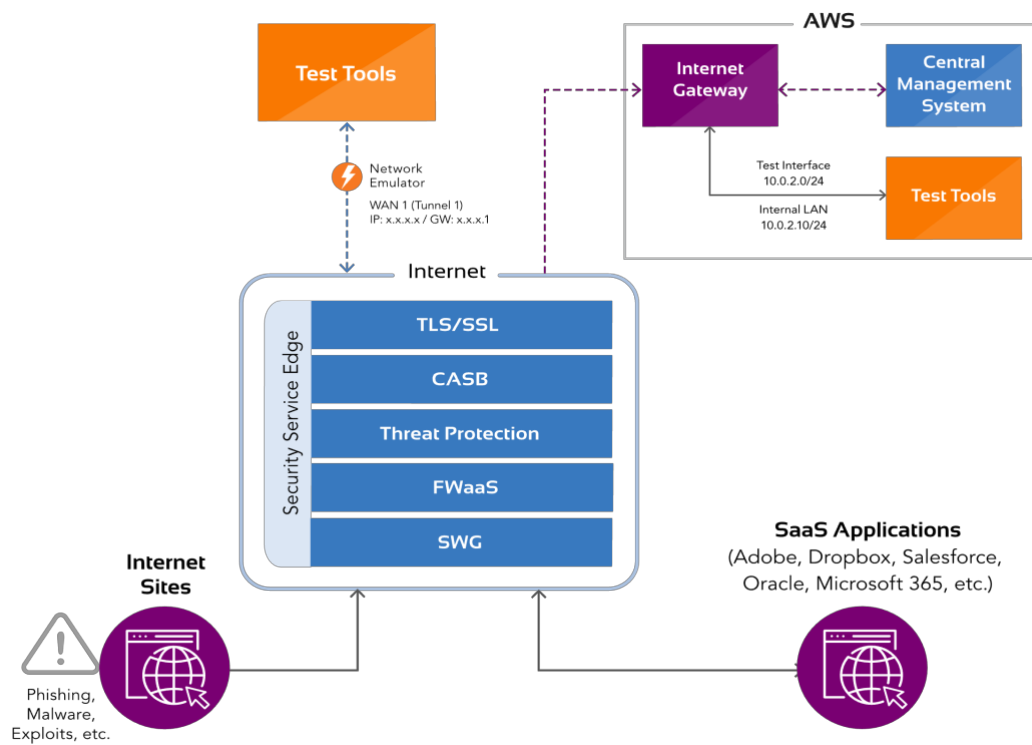
- Future evolving standards

Security Service Edge (SSE)

SSE technology is tested by creating a simulated multi-node enterprise network with each node having specific traffic and performance characteristics. Certification steps through various use cases for SaaS, IaaS applications and Internet Sites. Testing is based on MEF W162 SSE Test and Certification Requirements Specification.

SSE policies are applied, and SSE is tested:

- Threat Protection (evasion, exploits and malware)
- TLS/SSL Functionality
- Scalability Performance
- Classification Verification
- Conformance to MEF 117 SASE Service Attributes and Service Framework and MEF 138 Security Functions for IP Services
- Future evolving standards

Zero Trust

Zero Trust technology is tested by creating a simulated multi-node enterprise network with each node having specific traffic and performance characteristics. Certification steps through various use cases. Testing is based on MEF W163 Zero Trust Test and Certification Requirements Specification.

Zero Trust policies are applied, and Zero Trust is tested:

- Access Control
- Authentication
- Authorization
- Policy
- Change Control
- Reporting Capabilities, including logs and reports.
- TLS/SSL Functionality
- Scalability Performance
- Cloud Access/Application Control
- Conformance to MEF 118 Zero Trust Framework for MEF Services
- Future evolving standards
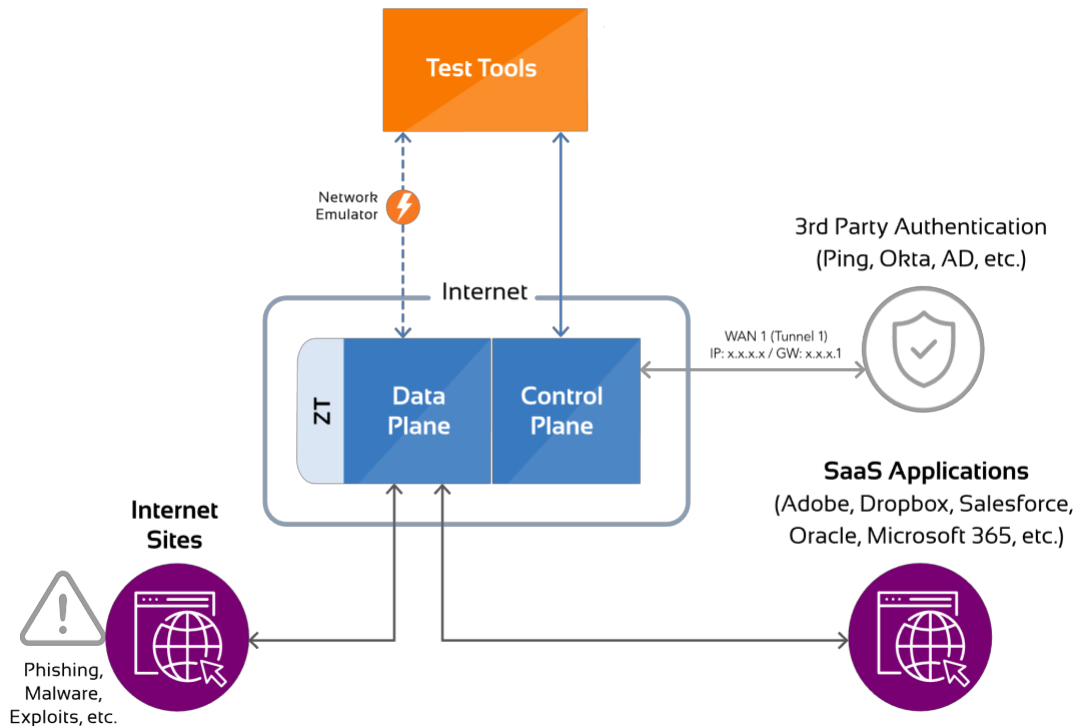
Powered by KEYSIGHT Ospirent

Secure Access Service Edge (SASE)

SASE technology receives a SASE certification when the technology provider has achieved certification in SD-WAN, SSE, and Zero Trust. The SASE score and rating are based on an average of the three individual certifications (SD-WAN, SSE, and Zero Trust).

Badges and Report Cards

Badges with attributes will appear in the [MEF Technologies Certification Registry](#) with ratings and additional details, including:

- Technology Provider Name (full legal name, if applicable)

- Hardware Family/Software Version

- Type of Certification

- Rating

- Date Tested

After the completion of each testing session, MEF issues a report card to the technology provider based on the results of the testing. The report card contains the overall rating (AAA-D), pass/fail for MEF certification, and the score in each category of the testing. The scores from each category are calculated based on 800 points, with penalties deducted for each test where appropriate, thus resulting in a score per category. The category scores are averaged, determining the overall score. This is shown in the example report card table below.

Example Technology Provider Report Cards:

MEF 3.0 Certified

Software-Defined Wide Area Network (SD-WAN)

Overall Score (AAA-D)	AAA
Vendor Name	
Certification Date	
Hardware Model	
Software Version	
Routing and Access Control	AAA
SWVC Application Assurance	AAA
SWVC Stability and Reliability	AAA
UCS Impairment	AAA
SWVC Performance	894 Mbps
Video MOS	4.35
Audio MOS	4.40

MEF 3.0 Certified

Security Service Edge (SSE)

Overall Score (AAA-D)	AAA
Vendor Name	
Certification Date	
Hardware Model	
Software Version	
SSL/TLS Decryption	AAA
Management Capabilities	AAA
Reporting Capabilities	AAA
Threat Prevention	AAA
Evasions	AAA
Throughput	Value
Threat Protection Score	Value
Evasion Defense Score	Value

Technology Provider SD-WAN Report Card Example   Technology Provider SSE Report Card Example

Technology Provider Zero Trust Report Card Example

A technology provider can certify different SD-WAN, SSE, Zero Trust, or SASE service offerings utilizing different hardware models or different software revisions.

Once a technology provider has successfully passed MEF Certification, CyberRatings.org will communicate the Report Card to MEF; MEF will create the MEF Certification Badge and present it to the technology provider. At the technology provider's discretion, the MEF Certification is updated on the MEF Technologies Certification Registry. Badges can be updated, at the technology provider's discretion, with new ratings every time a technology provider reruns their tests via the Continuous Integration/Continuous Test (CI/CT) process. The technology provider determines which certification is updated by the new certification.

Scoring and Rating

The scoring and rating system is based on a rating from D (lowest) |to AAA (highest). Tests performed for SD-WAN, SSE, Zero Trust, and SASE are based on a score from 0-to-800-points. Each category of testing begins with the allocation of 800 points. Points are then deducted when the device under test does not perform as specified.

The scores for each category of testing are then averaged to provide the overall rating. The SASE Certification Final Rating is an average of the SD-WAN Certification Rating, the SSE Certification Rating, and the Zero Trust Certification Rating.

Rating	Minimum Points	Maximum Points
AAA	775	800
AA	720	774
A	660	719
BBB	590	659
BB	540	589
B	480	539
CCC	420	479
CC	360	419
C	300	359
D	0	299

Deliverables

Items provided to the technology provider upon certification include:

- Certification rating badge associated with the report card.
- Listing of the certification in the MEF Technologies Certification Registry.
- MEF Certification marketing kit.

MEF Membership	MEF Certification Contract	Introduction to CyberRatings.org	Test schedule confirmed.	Execution and completion of testing.	Issuance of MEF promotional tools

Engagement Process

- Technology provider becomes a MEF member.
- Complete the MEF Certification contract and payment.
- Introduction to CyberRatings.org.
- Test schedule confirmed.
- Initial setup; the technology provider provides an engineer to architect the initial setup for certification.
- Execution and completion of testing.
- Issuance of report card, badge, marketing kit, and technical inclusion in MEF registries.