MPLIFY

Testing Guide

Zero Trust Certification Blueprint

August 2025 | Version 1.0

Contents

Figures

Introduction

This document specifies the Zero Trust 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 118 *Zero Trust Framework for MEF Services*
- MEF 163 *Draft R3 Zero Trust Certification Test Cases and Requirements*

Scope

Zero Trust Certification includes the following test categories:

- Policy Enforcement
- Access Control
- Authentication and Identity
- Zero Trust Network Access
- TLS/SSL Functionality

Out of scope:

Management and orchestration of Zero Trust Services, LSO APIs and IP forwarding paradigms other than longest prefix match-based forwarding.

Zero Trust Certification Framework

The Zero Trust Certification Framework is composed of the following five parts:

1. Test Cases & Requirements
2. Topology
3. Scoring Penalties
4. Scoring Methodology
5. Scoring Example

1. Test Cases & Requirements

Category: Policy Enforcement			
Description	**Zero Trust Requirement ID**	**TC & R Reference**	**Scoring Impact**
All Policy-Based Access Control Decisions MUST use one or more Policies to decide if access is granted.	MEF 118 R61	MEF 163 Draft R3 9.2.3	Yes
When a PBAC Policy, used by a Service that uses this Zero Trust Framework, uses Constrained RBAC (RBAC level 2), SoD MUST be enforced.	MEF 118 R86	MEF 163 Draft R3 9.1.1	Yes

Category: Access Control			
Description	**Zero Trust Requirement ID**	**TC & R Reference**	**Scoring Impact**
This test validates that the Zero Trust Implementation correctly identifies and allows authorized Subject User, Device, or Application to access permitted Target User, Device, or Application.	-	MEF 163 Draft R3 8.12.1	Yes
This test validates that the Zero Trust Implementation correctly identifies and blocks unauthorized Subject Users, Devices, and Applications from accessing specific Target Users, Devices, or Applications.	-	MEF 163 Draft R3 8.12.2	Yes
Only one of the following Policy Actions MUST be applied when a Policy Criterion is matched: • Allow • Block	MEF 118 R56	MEF 163 Draft R3 8.12.1, 8.12.2	Yes

Category: Authentication and Identity			
Description	**Zero Trust Requirement ID**	**TC & R Reference**	**Scoring Impact**
If the Identity Provider (IdP) is provided by the Subscriber, the IdPID MUST be reachable via its IP address.	MEF 118 R3	MEF 163 Draft R3 8.12.1, 9.2	Yes
If the IdP is external to the Subscriber, the IdPID MUST be reachable and publicly resolvable.	MEF 118 R4	MEF 163 Draft R3 8.12.1, 9.2	Yes
When the Service Provider is the IdP and SAML is used, SAML 2.0 MUST be used as the protocol for Authentication and Authorization.	MEF 118 R11	MEF 163 Draft R3 8.12.3	Yes
A Subject Actor authenticated by the IdP, MUST have at least one Role agreed for it as defined in the User Roles Service Attribute, Device Roles Service Attribute, and Application Roles Service Attribute.	MEF 118 R12	MEF 163 Draft R3 8.12.5, 9.1.1	Yes
The UserCommonName MUST be assigned one of the following values: • Null (meaning that no UserCommonName value is provided) • String of the name of the User	MEF 118 R27	MEF 163 Draft R3 8.12.3	Yes
The Service Provider MUST ensure that each User Actor is assigned at least one Role.	MEF 118 R30	MEF 163 Draft R3 9.1.1	Yes
The UserRoleCommonName MUST use one of the following values: • Null (meaning that no UserRoleCommonName value is provided) • String of the name of the User Role	MEF 118 R32	MEF 163 Draft R3 9.1.1	Yes
A Service Provider that adopts a Zero Trust Framework MUST ensure that at least one User Actor has the Role of System Administrator.	MEF 118 R34	MEF 163 Draft R3 8.12.4	Yes
The Service Provider and Subscriber MUST agree which Actor or Actors are assigned the Role of System Administrator	MEF 118 R35	MEF 163 Draft R3 8.12.4	Yes

Category: Zero Trust Network Access			
Description	**Zero Trust Requirement ID**	**TC & R Reference**	**Scoring Impact**
This test determines if Zero Trust policies allow remote users access to "hidden" networks.	-	Industry Best Practice 1	Yes
This test determines if Zero Trust policies have the granularity of IP address, identity, port, and protocol to restrict access to "hidden" networks.	-	Industry Best Practice 2	Yes
This test determines if Zero Trust policies restrict access to internal networks from clients on the Internet.	-	Industry Best Practice 3	Yes
This test determines if Zero Trust policies restrict lateral movement of remote users.	-	Industry Best Practice 4	Yes
This test determines if Zero Trust policies have granularity for only web-based applications or if the Zero Trust policies support non-web-based applications.	-	Industry Best Practice 5	Yes

Category: TLS/SSL Functionality			
Description	**Zero Trust Requirement ID**	**TC & R Reference**	**Scoring Impact**
To comply with this Zero Trust Framework, the Service Provider MUST encrypt all Service Attribute parameters and their respective values defined in MEF 118, both at rest and in transit, using common cryptographic suites.	MEF 118 R1	MEF 163 Draft R3 9.1.1	Yes

2. Topology

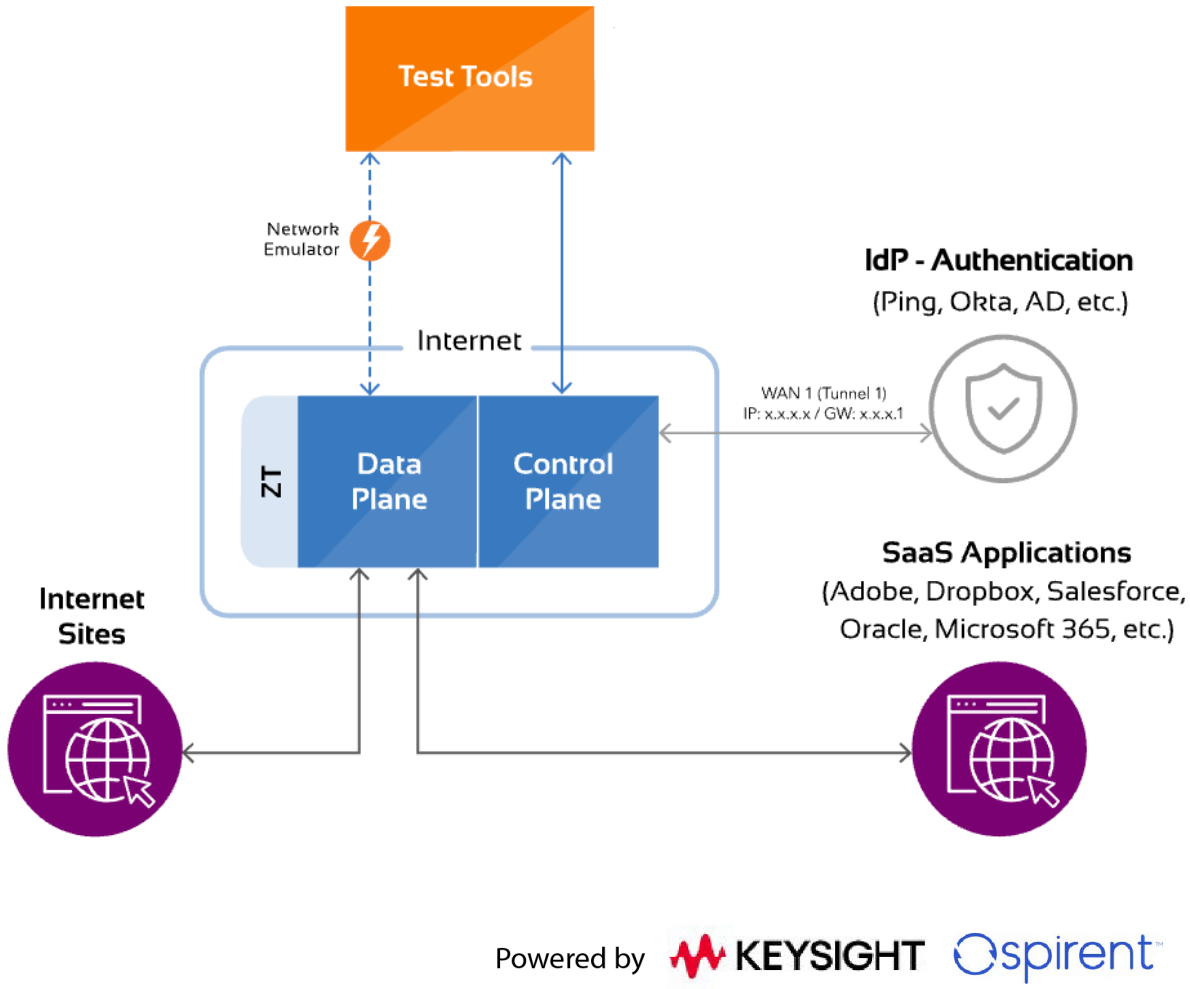

Figure 1 – Zero Trust Certification Topology

3. Scoring Penalties

Penalties: Policy Enforcement			
Section	**TC & R Reference**	**Description**	**Penalty**
1	MEF 163 Draft R3 9.2.3	Unrestricted Traffic Test (Allow All)	50%
2	MEF 163 Draft R3 9.1.1	Segmented Traffic Test	50%

Note 1: A Penalty applies to any test case failed within a given TC & R Reference section

Note 2: Policy Enforcement tests account for 15% of the Overall Score

Penalties: Access Control			
Section	**TC & R Reference**	**Description**	**Penalty**
1	MEF 163 Draft R3 8.12.1, 8.12.2	Overlapping Subnets: cyberratings.org and nsslabs.com	5%
2	MEF 163 Draft R3 8.12.1, 8.12.2	Overlapping Subnets: Source IP Address	20%
3	MEF 163 Draft R3 8.12.1, 8.12.2	Overlapping Subnets: Destination IP Address	20%
4	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: HTTP	5%
5	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: HTTPS	5%
6	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: FTP	5%
7	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: ICMP	5%
8	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: SSH	5%
9	MEF 163 Draft R3 8.12.1, 8.12.2	Network Services: SMTP	5%
10	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Facebook	1%
11	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Instagram	1%
12	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: LinkedIn	1%

Penalties: Access Control			
Section	**TC & R Reference**	**Description**	**Penalty**
13	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: X (formerly Twitter)	1%
14	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: TikTok	1%
15	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Netflix	1%
16	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: YouTube	1%
17	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Prime Video	1%
19	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Disney+	1%
20	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Microsoft Teams	1%
21	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Zoom	1%
22	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Google Meet	1%
23	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: WebEx	1%

Penalties: Access Control			
Section	**TC & R Reference**	**Description**	**Penalty**
24	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Skype	1%
25	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Microsoft OneDrive	1%
26	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Google Drive	1%
27	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: DropBox	1%
28	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: HTTP Webserver	1%
29	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: HTTPS Webserver	1%
30	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Gmail	1%
31	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Yahoo Mail	1%
32	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Outlook	1%
33	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Microsoft 365	1%
34	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Salesforce	1%
35	MEF 163 Draft R3 8.12.1, 8.12.2	Applications: Google Docs	1%

Note 1: A Penalty applies to any test case failed within a given TC & R Reference section

Note 2: Access Control tests account for 15% of the Overall Score

Penalties: Authentication and Identity			
Section	**TC & R Reference**	**Description**	**Penalty**
1	MEF 163 Draft R3 8.12.1, 8.12.3, 9.1.1, 9.2	Okta	20%
2	MEF 163 Draft R3 8.12.1, 8.12.3, 9.1.1, 9.2	Azure Active Directory	20%
3	MEF 163 Draft R3 8.12.4	Policy for Administrators (block https://discord.com)	20%
4	MEF 163 Draft R3 8.12.5	Policy for Regular Users (block https://wikipedia.org)	20%
5	MEF 163 Draft R3 8.12.5	Policy for Guest Users (block https://amazon.com)	20%

Note 1: A Penalty applies to any test case failed within a given TC & R Reference section

Note 2: Authentication and Identity tests account for 30% of the Overall Score

Penalties: Zero Trust Network Access			
Section	**TC & R Reference**	**Description**	**Penalty**
1	Industry Best Practice 1	Remote access to applications “hidden” networks	20%
2	Industry Best Practice 2	Access control of “hidden” networks	20%
3	Industry Best Practice 3	No inbound connections to private networks	20%
4	Industry Best Practice 4	Full Network access not automatically granted to remote users	20%
5	Industry Best Practice 5	Support for non-standard ports and non-web protocols	20%

Note 1: A Penalty applies to any test case failed within a given TC & R Reference section

Note 2: Zero Trust Network Access tests account for 25% of the Overall Score

Penalties: TLS/SSL Functionality			
Section	**TC & R Reference**	**Description**	**Penalty**
1	MEF 163 Draft R3 9.1.1	TLS_AES_256_GCM_SHA384 (0x13, 0x02)	10%
2	MEF 163 Draft R3 9.1.1	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)	10%
3	MEF 163 Draft R3 9.1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)	10%
3	MEF 163 Draft R3 9.1.1	TLS_AES_128_GCM_SHA256 (0x13, 0x01)	10%
5	MEF 163 Draft R3 9.1.1	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA8)	10%
6	MEF 163 Draft R3 9.1.1	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC0, 0x28)	10%
7	MEF 163 Draft R3 9.1.1	TLS_CHACHA20_POLY1305_SHA256 (0x13, 0x03)	10%
8	MEF 163 Draft R3 9.1.1	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xCC, 0xA9)	10%
9	MEF 163 Draft R3 9.1.1	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x2C)	10%
10	MEF 163 Draft R3 9.1.1	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2B)	10%

Note 1: A Penalty applies to any test case failed within a given TC & R Reference section

Note 2: TLS/SSL Functionality tests account for 15% of the Overall Score

4. Overall Scoring Methodology & Rating

The Zero Trust Certification Overall Score is calculated based on the credited percentages awarded in each category and category weight, as follows:

Zero Trust Certification Scoring Methodology		
Category	**Calculation**	**Weight**
Policy Enforcement	Calculated penalty percentage per section 3. 'Scoring Penalties'	15
Access Control	Calculated penalty percentage per section 3. 'Scoring Penalties'	15
Authentication and Identity	Calculated penalty percentage per section 3. 'Scoring Penalties'	30
Zero Trust Network Access	Calculated penalty percentage per section 3. 'Scoring Penalties'	25
TLS/SSL Functionality	Calculated penalty percentage per section 3. 'Scoring Penalties'	15

1. Credited percentage for Policy Enforcement = (100% - Penalty%) x 15 weight
2. Credited percentage for Access Control = (100% - Penalty%) x 15 weight
3. Credited percentage for Authentication and Identity = (100% - Penalty%) x 30 weight
4. Credited percentage for Zero Trust Network Access = (100% - Penalty%) x 25 weight
5. Credited percentage for TLS/SSL Functionality = (100% - Penalty%) x 15 weight
6. Total Credited Percentage = Credited percentage for Policy Enforcement + Credited percentage for Access Control + Credited percentage for Authentication and Identity + Credited percentage for Zero Trust Network Access + Credited percentage for TLS/SSL Functionality
7. Zero Trust Certification final rating is determined based on the Total Credited percentage – Overall Score, as per the Zero Trust Certification Rating table below

Zero Trust 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%

5. Overall Scoring Example

The following example demonstrates the calculation of a Zero Trust Certification overall score and final rating.

Category	Calculated Penalty	Weight
Policy Enforcement	0%	15
Access Control	5%	15
Authentication and Identity	0%	30
Zero Trust Network Access	0%	25
TLS/SSL Functionality	0%	15

In this example, the calculation for the Zero Trust Certification overall score and final rating is as follows:

Policy Enforcement	((100% – 0%) × 15 Weight) = 15%
Access Control	((100% – 5%) × 15 Weight) = 14.25%
Authentication and Identity	((100% – 0%) × 30 Weight) = 30%
Zero Trust Network Access	((100% – 0%) × 25 Weight) = 25%
TLS/SSL Functionality	((100% – 0%) × 15 Weight) = 15%

Overall Score:	(15% + 14.25% + 30% + 25% + 15%) = 99.25%
Final Rating:	AAA

Revision History

Revision History	Date	Revision
Version 1.0	August 1, 2025	Zero Trust Certification Blueprint Version 1.0

Testing Guide: Zero Trust Certification Blueprint v1.0