Draft Standard

MEF 163 Draft (R1)

Zero Trust Certification Test Cases and Requirements

September 2023

This draft represents MEF work in progress and is subject to change.

This draft document represents MEF work in progress; it has not achieved full MEF standardization and is subject to change. Changes are likely before this becomes a fully endorsed MEF Standard. The reader is strongly encouraged to keep this in mind and review the Release Notes (if applicable) when making a decision on adoption. Additionally, because this document has not been adopted as a Final Specification in accordance with MEF's Bylaws, Members are not obligated to license patent claims that are essential to implementation of this document under MEF's Bylaws.

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and MEF Forum (MEF) is not responsible for any errors. MEF does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by MEF concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by MEF as a result of reliance upon such information.

The information contained herein is intended to be used without modification by the recipient or user of this document. MEF is not responsible or liable for any modifications to this document made by any other party.

The receipt or any use of this document or its contents does not in any way create, by implication or otherwise:

a) any express or implied license or right to or under any patent, copyright, trademark or trade secret rights held or claimed by any MEF member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any MEF members will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor

c) any form of relationship between any MEF member and the recipient or user of this document.

Implementation or use of specific MEF standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in MEF Forum. MEF is a non-profit international organization to enable the development and worldwide adoption of agile, assured and orchestrated network services. MEF does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

The following members of the MEF participated in developing this document and have requested to be included in this list.

Editor Note 1: This list will be finalized before Letter Ballot. Any member that comments in at least one CfC is eligible to be included by opting in before the Letter Ballot is initiated. Note it is the MEF member listed here (typically a company or organization), not their representatives.

2 Abstract

A Zero Trust Framework (ZTF), defined in MEF 118 [5], is a cybersecurity architecture where users or clients (end users, applications, and other nonhuman Users, Devices, and Applications that request information from resources) are authenticated, authorized, and continuously validated before being granted access to, maintaining access to, or performing operations on applications.

The focus of this document is on the test cases and requirements for certification of Zero Trust (ZT) implementations. The certification of ZT implementation seen as key for enterprise customers to know about different offerings and solutions so that they can make informed decisions when purchasing ZT.

3 Release Notes

This document is currently out for Call for Comments Ballot number 2. All comments from Call for Comments Ballot 1 have been discussed and resolved except where noted in Table 1 below.

Release Note Topic	Section(s) Impacted	Comments
The Terminology and Abbreviations will be updated in a future revision of the document.	4	
We agreed to add private applications to the test configuration after the Beta test is completed.	7.2.1	
Private applications which include customer applications will be added after the Beta is completed.	8.3	
Cloud-to-cloud will be added here after the Beta is completed.	8.6	
The ability to export a report in a file format like .pdf, .csv, etc. will be added after the Beta is completed.	10	
The test methodology is still being discussed for rows in Table 6 with a Test Methodology Required methodology. Once finalized, the test methodology will be updated.	11	
There is an ongoing discussion on certification and rating. The text in section 12.1, as well as other text within this document is subject to change based on the results of the discussion.	12.1	

Table 1 – Release Notes

4 Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions of terms are found in other documents. In these cases, the third column provides references controlled in other MEF or external documents.

In addition, terms defined in MEF 118 [5] and MEF 162 [6] are included in this document by reference and are not repeated in the table below.

Term	Definition	Reference
Management Capabilities	The set of functions that allow management of a Zero Trust implementation.	This document
Reporting Capabilities	The set of functions that support reporting from a Zero Trust implementation.	This document

Table 2 – Terminology

Abbreviation	Definition	Reference
DUT	Device Under Test	This document
FTP	File Transfer Protocol	This document
PKI	Public Key Infrastructure	This document

Table 3 – Abbreviations

Editor Note 2: The Terminology and Abbreviations will be updated in a future revision of the document.

5 Compliance Levels

The key words "**MUST**," "**MUST NOT**," "**REQUIRED**," "**SHALL**", "**SHALL NOT**", "**SHOULD**", "**SHOULD NOT**", "**RECOMMENDED**", "**NOT RECOMMENDED**", "**MAY**", and "**OPTIONAL**" in this document are to be interpreted as described in BCP 14 (RFC 2119 [1], RFC 8174 [3]) when, and only when, they appear in all capitals, as shown here. All keywords must be in bold text.

Items that are **REQUIRED** (contain the words **MUST** or **MUST NOT**) are labeled as **[Rx]** for required. Items that are **RECOMMENDED** (contain the words **SHOULD** or **SHOULD NOT**) are labeled as **[Dx]** for desirable. OPTIONAL items (containing the words **MAY** or **OPTIONAL**) are labeled as **[Ox]** for optional**.**

Editor Note 3: The following paragraph will be deleted if no conditional requirements are used in the document.

A paragraph preceded by **[CRa]<** specifies a conditional mandatory requirement that **MUST** be followed if the condition(s) following the "<" have been met. For example, "**[CR1]<**[D38]" indicates that Conditional Mandatory Requirement 1 must be followed if Desirable Requirement 38 has been met. A paragraph preceded by **[CDb]<** specifies a Conditional Desirable Requirement that **SHOULD** be followed if the condition(s) following the "<" have been met. A paragraph preceded by **[COc]<** specifies a Conditional Optional Requirement that **MAY** be followed if the condition(s) following the "<" have been met.

6 Numerical Prefix Conventions

Editor Note 4: This section will be deleted if no numerical prefixes are used in the document.

This document uses the prefix notation to indicate multiplier values, as shown in Table 4.

Decimal		**Binary**	
Symbol	**Value**	**Symbol**	**Value**
k	10^3	Ki	2^{10}
M	10^6	Mi	2^{20}
G	10^9	Gi	2^{30}
T	10^{12}	Ti	2^{40}
P	10^{15}	Pi	2^{50}
E	10^{18}	Ei	2^{60}
Z	10^{21}	Zi	2^{70}
Y	10^{24}	Yi	2^{80}

Table 4 – Numerical Prefix Conventions

7 Introduction

A Zero Trust Framework (ZTF), defined in MEF 118 [5], is a cybersecurity architecture where users or clients are authenticated, authorized, and continuously validated before being granted access to, maintaining access to, or performing operations on applications.

The focus of this document is on the test cases and requirements for certification of Zero Trust (ZT) implementations. The certification of ZT implementation seen as key for enterprise customers to know about different offerings and solutions so that they can make informed decisions when purchasing ZT.

The testing defined within this document is intended to provide a rating, from D (lowest) to AAA (highest). Ratings are determined based on the results of the test cases defined in this document. For example, a ZT implementation that supports more Policies will be rated higher than a ZT implementation that only supports a limited number of Policies. Ratings are based on weighting applied to each section of the test requirements in this document. See section 12 for more details on the rating methodology for ZT implementation.

After the completion of testing, an overall rating is provided. This overall rating of a ZT implementation can be used to compare different ZT Vendor's ability to meet the test requirements and, therefore, the requirements of Service Providers and enterprise customers. In the same manner, Service Provider's offerings can be compared to determine how different offerings address the end customer's requirements.

In addition to providing an overall rating, a MEF Certification is provided. This MEF Certification is based on compliance with MEF standards tested using the test methodologies defined in section 11.

The testing defined within this document is intended to be repeatable to cover new software releases, service configurations, or updates to how a ZT implementation is managed. Continuous Integration/Continuous Deployment (CI/CD) strategies for MEF certification are being defined in the same manner as in MEF W90.2 [4]. Repeating the process allows ratings to increase or decrease based on the performance of an implementation or service during continued testing. One release may be certified, while another release may fail certification testing. If a new software release breaks a critical function. In that case, this can be identified during repeated certification testing, and the rating adjusted accordingly. In the same way, if a new software release provides fixes for shortfalls identified in previous certification testing, the rating can be increased accordingly.

7.1 Zero Trust

The increased usage of cloud services, mobile devices, work-from-home employees, shadow IT, and the Internet of Things (IoT) has dissolved traditional network perimeters. Services must evolve to provide secure User, Device, and Application access to the Subscriber's networked resources (referred to as Target Actors in this document) from any location, including interactions with third-party organizations, e.g., business partners, contractors, etc.

A Zero Trust cybersecurity approach removes the assumption of trust from these Users, Applications, and Devices (referred to as Actors in this document). It focuses on accessing Target

Actors in a secure and authorized manner, enforcing rigorous access controls, and continually inspecting, monitoring, and logging network activity from the different Subject Actors. This requires data-level protections, a robust id Users, Devices, and Applications architecture, and strategic micro-segmentation to create granular trust zones around a Subscriber's digital resources.

Zero Trust evaluates access requests and network traffic behaviors in real time over the length of active Sessions while continually and consistently recalibrating Subject Actor access to Target Actors and associated Policy Actions.

The above paragraphs are taken from MEF 118 [5].

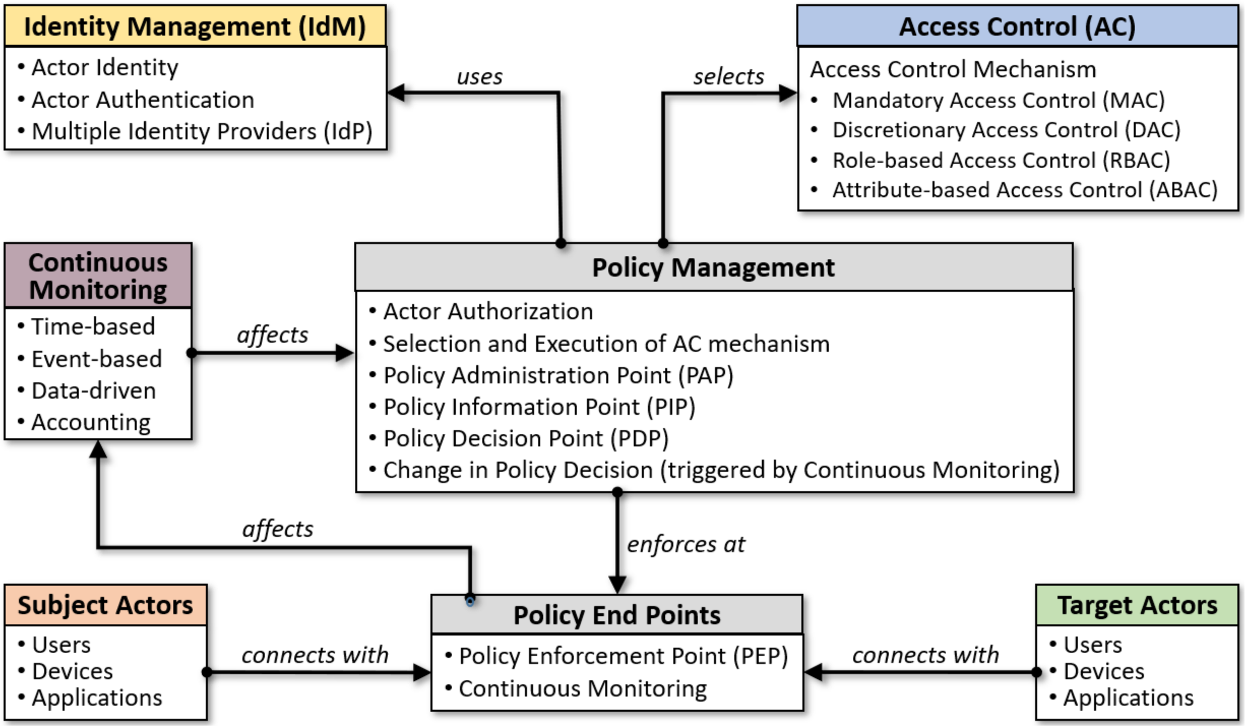
Identity Management (IdM)
• Actor Identity
• Actor Authentication
• Multiple Identity Providers (IdP)
uses
selects
Access Control (AC)
Access Control Mechanism
• Mandatory Access Control (MAC)
• Discretionary Access Control (DAC)
• Role-based Access Control (RBAC)
• Attribute-based Access Control (ABAC)
Continuous Monitoring
• Time-based
• Event-based
• Data-driven
• Accounting
affects
Policy Management
• Actor Authorization
• Selection and Execution of AC mechanism
• Policy Administration Point (PAP)
• Policy Information Point (PIP)
• Policy Decision Point (PDP)
• Change in Policy Decision (triggered by Continuous Monitoring)
affects
enforces at
Subject Actors
• Users
• Devices
• Applications
connects with
Policy End Points
• Policy Enforcement Point (PEP)
• Continuous Monitoring
connects with
Target Actors
• Users
• Devices
• Applications

Figure 1 – ZT Framework

Figure 1, taken from MEF 118 [5], reflects how Policy is used to manage the ZTF. Policy Management includes Users, Devices, and Applications Authorization, the Policy Administration Point functionality, the Policy Information Point functionality, and the Policy Decision Point functionality. Policy End Points are responsible for Policy Enforcement Point functionality and use information from Continuous Monitoring to make Policy decisions. For more detail on the ZT Framework, see MEF 118 [5].

7.2 What will be tested?

The certification described in this document is designed to address the challenges faced by security and IT professionals in selecting and managing security products. The scope of the test methodologies in this document includes the following capabilities, which are considered essential in any ZT offering:

- Policy Enforcement and Access Control

- Authentication via integration with Id Users, Devices, and Applications Providers (IdP)
- Reporting Capabilities
- Management Capabilities

7.2.1 Test Configuration

The test configuration used to perform testing of ZT implementation is shown in Figure 2.

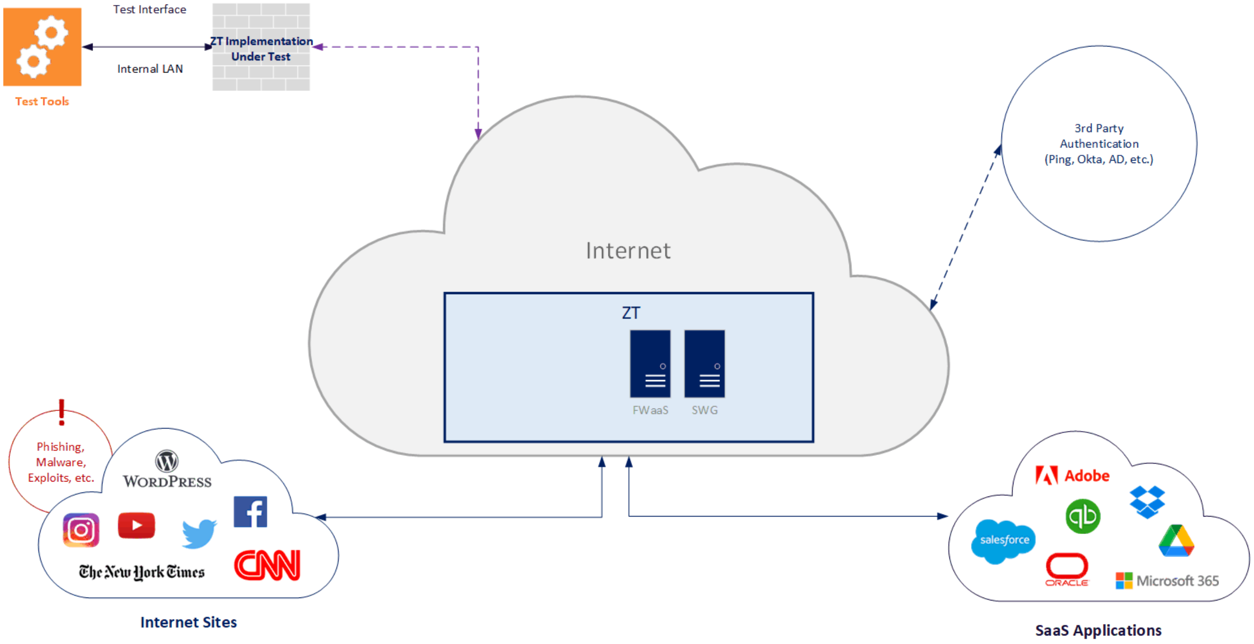

Figure 2 – Test Configuration for ZT

Figure 2 reflects the ZT functions within a single implementation that provides Authentication and Authorization. The tests outlined in the remainder of this document use this basic configuration.

Note: There may be slight modifications to this test configuration for specific tests.

8 Policy Enforcement

The ZT implementation should be able to securely route or forward traffic through the cloud service via policy either on-prem or cloud-based policy enforcement, via commonly accepted tunnel methods supported by routers and firewalls, and/or via an agent deployed on a desktop, laptop, or mobile device. Test traffic includes a typical enterprise campus environment and data center content.

A Policy defines the type of rules, conditions, and constraints for a Service. A system that implements Policies utilizes the following Policy functions:

Policy Administration Point (PAP): an entity that is responsible for configuration and maintenance of all other functional entities that make up a Policy

Policy Information Point (PIP): a repository that contains generic information used by Policies. Examples include Session, geolocation, reputation, and risk calculation data, and associated metadata.

Policy Decision Point (PDP): an entity that evaluates an access request using a set of Evaluation Policies, along with applicable information from the PIP. The term “Evaluation Policies” may include Authorization Policies, as well as more robust mechanisms (e.g., RBAC or ABAC) that provide a binary response (i.e., permit or deny access) to send to the PEP. Put another way, the PDP decides whether to Authorize the Actor based on applicable information.

Policy Enforcement Point (PEP): An entity that implements Policy decisions that were made by the PDP. The PEP receives an access request and forwards this request to the PDP. When the PEP receives the response from the PDP, the PEP implements that Policy decision.

8.1 Policy Actions

Policy Actions apply to a Subject Actor wanting to access a specific Target Actor. The Policy Actions may change triggered by the passage of a predetermined amount of time, or an Event-based on the continuous monitoring of the Actors and the corresponding Session. Refer to MEF 118 [5] for Events created during continuous monitoring that can trigger a change in Policy Actions.

[R1] The test **MUST** validate when a Policy Criterion is matched on the Allow List the Policy Action is Allow.

[R2] The test **MUST** validate when a Policy Criterion is matched on the Block List the Policy Action is Block.

The “Allow” Policy Action means that for a given Session between a specific Subject Actor and Target Actor, the Policy End Point permits the Subject Actor to send all IP Packets to the Target Actor and the receive IP Packets from the Target Actor for which Policies are applied.

The “Block” Policy Action means that for a given Session, between a specific Subject Actor and Target Actor, the Policy End Point denies the Subject Actor from sending any IP Packets to the

Target Actor and denies the receipt of IP Packets from the Target Actor for which Policies are applied.

8.2 Policy End Points

A Policy End Point is a location where one or more Policy-related functions are placed. Policies are executed (via PEP) and monitored at a Policy End Point. A Policy End Point is placed at locations where practical when implementing a Zero Trust Framework. Policy End Points are optimally placed in a Device or Application Actor. However, this may not be practical, e.g., inside an IoT Device with minimal processing capability, in which case the Policy End Point would be placed as close as possible to the Actor. Furthermore, a Subject Actor may be able to reach different Target Actors via different networks. Therefore, a Policy End Point must be placed at each access point where the Subject Actor can reach the Target Actor to ensure that Policies can be effectively applied. Example use cases for the placement of Policy End Points is illustrated in MEF 118 [5].

[R3] The test **MUST** validate that a Zero Trust Framework provides a Policy End Point.

8.3 Access Control

As described in MEF 118 [5] policies are rules configured to permit or deny access from a user to an application using criteria such as source, destination, user/group, and service. Policies are typically written to permit, deny, or restrict network traffic to or from one or more of the following:

- **Unknown External Users, Devices, and Applications**— an external User, Device, or Application with unknown security (e.g., Internet web server).
- **Known 3rd Party Users, Devices, and Applications Services** — a service or application (e.g., Office 365, Google Docs, or Salesforce) the enterprise uses, and authorized users are permitted access.
- **Known Internal Users, Devices, and Applications**– an internal User, Device, or Application, i.e., a User, Device, or Application that is being secured and protected.

This test section verifies that the Device Under Test (DUT) enforces Zero Trust policies over a range of policy environments, from simple to complex. The tests incrementally build on a baseline consisting of a simple configuration with no policy restrictions – to a complex multiple-zone configuration that supports many users, networks, policies, and applications. Traffic will be tested at each level of complexity, ensuring specified policies are enforced. For the three use cases (User on site, Remote user, Third-party user), testing will confirm that authorized traffic from a Subject Users, Devices, and Applications to a Target Users, Devices, and Applications is allowed while unauthorized traffic between them is blocked.

Note: The protocols and applications shown are examples. The protocols and applications that are included in testing will be provided by the test house as a part of the test agreement.

The policies are described in the following sections.

8.4 Basic Internet Services

Policies are created that allow the following basic Internet services.

- An outbound rule allowing access to at least three of these basic Internet services
  - HTTP
  - HTTPS
  - DNS
  - SMTP
  - IMAP
  - POP3
  - Exchange/MAPI
  - FTP

8.5 Trusted Third Party

Policies are created as described for these trusted third-party applications.

- Allow and Deny (Deny all, Allow all, Deny individual applications)Subject User, Device, or Application (internal and remote) connectivity to at least three of these trusted third-party Target User, Device, or Application
  - Office 365
  - Salesforce
  - NetSuite
  - Google Workspace
  - Dropbox

8.6 Location Access

Policies are created as described for these locations.

- Allow and Deny (Deny all, Allow all, Deny individual locations) Subject User, Device, or Application at one location access to the Target User, Device, or Application at another location
  - Enterprise Site secure connectivity

  - Enterprise Site to Cloud resources

8.7 Connectivity

Policies are created as described for connectivity.

- Allow/Deny remote/mobile Subject Users, Devices, and Applications secure connectivity to the Target Users, Devices, and Applications
  - Enterprise Site
  - Cloud resources

8.8 Social Media

Policies are created as described for social media.

- Allow/Deny Subject Users, Devices, and Applications (Deny all, Allow all, Deny individual social media applications and websites) access to Target Users, Devices, and Applications supporting popular social networking applications and websites
  - Top 10 social media applications, including Facebook, Twitter, LinkedIn, Glassdoor, or other Web applications

Note: The top 10 social media applications will be updated every six months.

8.9 Video and Voice Teleconferencing

Policies are created as described for Video and Voice teleconferencing.

- Allow/Deny (Deny all, Allow all, Deny individual teleconferencing applications) Subject Users, Devices, and Applications access to at least two Target Users, Devices, and Applications supporting Video and Voice teleconferencing
  - Microsoft Teams
  - Zoom
  - Cisco WebEx
  - Google Meet

8.10 Streaming Media

Policies are created as described for streaming media applications and web sites.

- Allow/Deny (Deny all, Allow all, Deny individual applications and websites) Subject Users, Devices, and Applications access to at least three Target Users, Devices, and Applications supporting streaming media applications and websites

  - Netflix
  - Prime Video
  - Hulu
  - YouTube
  - TikTok
  - HBO Max
  - Disney+
  - AppleTV

8.11 Deny by Default

Policies are created as described to block traffic that has not be allowed.

- A deny-by-default action that blocks all traffic from Subject Users, Devices, and Applications to Target Users, Devices, and Applications that has not been explicitly allowed.

8.12 Policy Enforcement Test Cases

The test cases that use the policies created above are in the following sections.

8.12.1 Enable Authorized Access / Applications

Test Objective: The ZT implementation's PEP should correctly identify and allow authorized Subject User, Device, or Application to access permitted Target User, Device, or Application.

Test Process: Testing the PEP for each of the policy areas above determines whether all transmitted traffic that adhered to policies reached its intended destinations and whether all transmitted traffic that violated policies was blocked.

[R4] When Subject Users, Devices, or Applications have been permitted access to Target Users, Devices, or Applications, the test **MUST** determine if traffic from the Subject Users, Devices, and Applications to the Target Users, Devices, and Applications passes correctly.

8.12.1.1 Scoring Penalty

The scoring penalty for section 8.12.1 is 100%.

8.12.2 Block Unauthorized Access to Target Users, Devices, and Applications

Test Objective: The ZT implementation's PEP should correctly identify and block an unauthorized Subject Users, Devices, and Applications from accessing specific Target Users, Devices, or Applications.

Test Process: Testing of the PEP for each policy area above determines whether all transmitted traffic that adhered to policies reached their intended destinations and whether all transmitted traffic that violated policies was blocked.

[R5] When Subject Users, Devices, or Applications have been permitted access to Target Users, Devices, or Applications, the test **MUST** determine if traffic from the Subject Users, Devices, and Applications destined to the Target Users, Devices, and Applications passes correctly.

[R6] When Subject Users, Devices, or Applications are not permitted access to Target Users, Devices, or Applications, the test **MUST** determine if traffic from the Subject Users, Devices, and Applications is blocked.

8.12.2.1 Scoring Penalty

The scoring penalty for section 8.12.2 is 100%.

8.12.3 Overlapping Subnets

Overlapping or identical subnets with an organization's infrastructure can present a configuration challenge when all the locations are combined and managed from a single cloud service. These conflicting RFC-1918 [1] private IP addresses can be a result of mergers and acquisitions, lax IT policies, or intentionally assigned as a "cookie-cutter" style deployment (e.g., multiple franchise locations such as retail stores or chain restaurants).

Examples of policies include the following:

- Single location: There are overlapping IP subnets at the same location.
- Multiple locations: sites 1, 2, and 3. Each site is on an IP subnet identical to the other sites.
- Allow Subject User, Device, or Application at one location to access an Internet Target Users, Devices, and Applications (Office365) while denying Subject User, Device, or Application at another location access to the same Target Users, Devices, and Applications.
- Two Subject Users, Devices, or Applications that are using the same IP address can both access the same Target User, Device, or Application and receive the correct response from that Target User, Device, or Application.

Test Objective: Testing would determine whether all transmitted traffic from Subject User, Device, or Application that adhered to policies enforced in the PEP reached their intended Target User, Device, or Application regardless of multiple sites using overlapping address spaces.

Test Process: A Subject User, Device, or Application with an overlapping IP address requests access to a Target User, Device, or Application. It is verified that the correct Subject User, Device, or Application is given access to the Target User, Device, or Application by the PEP.

[R7] The test **MUST** verify that traffic is delivered to the correct Target Users, Devices, and Applications if multiple Subject Users, Devices, or Applications use the same IP subnet.

[R8] The test **MUST** verify that if multiple Subject Users, Devices, or Applications use the same IP subnet, one Subject Users, Devices, and Applications can be permitted access to a Target Users, Devices, and Applications. In contrast, others are denied access to the same Target Users, Devices, and Applications.

8.12.3.1 Scoring Penalty

The scoring penalty for section 8.12.3 is 25%.

8.12.4 Security Assertion Markup Language Authentication for Subject Users, Devices, and Applications

Test Objective: Testing verifies that Security Assertion Markup Language (SAML) interoperability across popular identity providers.

Test Process: The test process is to configure SAML authentication to one or more if the following Identity providers:

- Okta
- Ping
- Azure Active Directory
- Local Active Directory

Verify that Subject Users, Devices, and Applications groups can be used to applied policies.

[R9] The test **MUST** verify if a new Subject Users, Devices, and Applications are added to a group and automatically gain the same access as others.

[R10] The test **MUST** verify that if an existing Subject Users, Devices, and Applications are removed from a group, they automatically lose access to Target Users, Devices, and Applications provided by the group.

8.12.4.1 Scoring Penalty

The scoring penalty for section 8.12.4 is 50%.

8.12.5 SAML Authentication for Administrators

Test Objective: Testing will verify if the implementation supports SAML authentication for administrator accounts logging in to the administrative portal.

Test Process: A Subject User, Device, or Application with an administrator Role accesses the administrative portal and is provided access.

[R11] The test **MUST** verify that a Subject Users, Devices, and Applications with an administrator Role can be authenticated via SAML when logging into the administrative portal.

8.12.5.1 Scoring Penalty

The scoring penalty for section 8.12.5 is 50%.

8.12.6 Identity Aware Policies

Test Objective: It is important that the identity of a Subject User, Device, or Application can be used to assign/associate policies to a subject User, Device, or Application. Testing will verify that the implementation's PEP enforces policies based on the identity of a Subject Users, Devices, and Applications.

Test Process: A Subject User, Device, or Application access a Target User, Device, or Application with authorization based on their identity by the PEP.

[R12] The test **MUST** verify that policies can be assigned/associated based on the Identify of a Subject Users, Devices, and Applications.

8.12.6.1 Scoring Penalty

The scoring penalty for section 8.12.6 is 50%.

9 Management Capabilities

A ZT implementation must provide comprehensive management control to accomplish the expected functionality. Further best practices in user experience should be fundamental to the associated interface. The ZT implementation will be assessed to determine if it meets the following requirements.

9.1 Authentication

9.1.1 Role-Based Access Control

Role-Based Access Control (RBAC) is defined in MEF 118 [5] as “A collection of access Authorizations a Subject or Target Users, Devices, and Applications receives based on a given set of Roles.”

Test Objective: This test verifies that RBAC is supported by creating Roles for Subject and Target Users, Devices, and Applications and ensuring that authentication is done correctly.

The System Administrator Role exists as a default Role per MEF 118 [5].

The set of Roles that are created by the System Administrator for the purpose of this testing are:

- Sales
- Marketing
- Accounting (Finance)
- Engineering (Networking/Web Development)
- User
- Super User
- Custom (a combination of two or more roles)

Test Process: The above Roles are created and then it is verified that the Role was created correctly.

[R13] The test **MUST** verify that the ZT implementation supports RBAC.

9.1.1.1 Scoring Penalty

The scoring penalty for section 9.1.1 is 100%.

9.1.2 Policy-Based Access Control Policies using MAC

Policy-based Access Control (PBAC) is defined in MEF 118 [5] as “an Access Control method that uses Policies to determine the appropriate type of Access Control based, e.g., MAC, DAC, RBAC, or ABAC, on the Subject and Target Actors’ Service Attributes and behavior, the current Situation, and applicable business requirements". The focus of this section is on PBAC using Mandatory Access Control (MAC).

Test Objective: The test verifies that PBAC policies using MAC provide the appropriate access by Subject Users, Devices, and Applications to Target Users, Devices, and Applications that are authorized.

Test Process: A Subject User, Device, or Application is authorized access to a specific Target User, Device, or Application. It is verified that the PBAC policy using MAC allows access to the authorized Target User, Device, or Application and cannot access an unauthorized Target User, Device, or Application.

[R14] The testing **MUST** verify that when PBAC policies using MAC are used, that the Security Label, if present, is used as an input to the Authorization process.

An unauthorized Target Users, Devices, and Applications is created on the solution under test.

[R15] The testing **MUST** verify that when PBAC policies using MAC are used, that a Subject User, Device, or Application cannot reach an unauthorized Target User, Device, or Application.

9.1.2.1 Scoring Penalty

If PBAC using MAC policies with security labels are supported, tested, and fail, the scoring penalty for section 9.1.2 is 100% .

9.1.3 PBAC Policies using Attribute-Based Access Control

The focus of this section is on PBAC using Attribute-based Access Control (ABAC).

Test Objective: The test verifies that PBAC policies using ABAC provide the appropriate access by Subject Users, Devices, and Applications to Target Users, Devices, and Applications that are authorized.

Test Process: A Subject User, Device, or Application is authorized access to a specific Target User, Device, or Application by:

- Assigning one or more Subject attributes to the Subject User, Device, or Application
- Assigning one or more Target attributes to the Target User, Device, or Application.

It is verified that the PBAC policy using ABAC allows:

- Allow access to the authorized Target User, Device, or Application
- Block access an unauthorized Target User, Device, or Application.

In addition, as described in MEF 118 [5], Environmental Conditions, referred to as Context within this document are included in PBAC using ABAC. Context examples are:

- Mobile
- Working from Home (WFH)
- In the office

Context is assigned to both Subject and Target Users, Devices, and Applications.

[R16] When configuring a test, all of the above ABAC attributes **MUST** be included in the test.

[R17] The testing **MUST** verify that when PBAC policies using ABAC are used, that a Subject User, Device, or Application can reach an authorized Target User, Device, or Application.

An unauthorized Target Users, Devices, and Applications is created on the solution under test.

[R18] The testing **MUST** verify that when PBAC policies using ABAC are used, that a Subject User, Device, or Application cannot reach an unauthorized Target User, Device, or Application.

9.1.3.1 Scoring Penalty

The scoring penalty for section 9.1.3 is 100%.

9.2 Policy

9.2.1 Policy Definition

The ZT implementation should allow the creation of policies used to control access, functionality, and behavior of a ZT implementation. See the list of policies to be created in section 8.

[R19] The test **MUST** verify that policies that describe the behavior of ZT implementations can be created.

9.2.1.1 Scoring Penalty

The scoring penalty for section 9.2.1 is 100%.

9.2.2 View Policy

The ZT implementation should provide the ability to identify what policy has been violated when an alert is generated.

[R20] The test **MUST** verify that when an alert is generated, the policy that has been violated is identified.

9.2.2.1 Scoring Penalty

The scoring penalty for section 9.2.2 is 50%.

9.2.3 Policy Association

The ZT implementation allows associating one or more policies with a Subject Users, Devices, and Applications or a Target Users, Devices, and Applications. Policies are created, as shown in section 8. Subject Users, Devices, and Applications are given access to different Target Users, Devices, and Applications based on their defined roles.

Roles	Target Users, Devices, and Applications
Sales	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Salesforce, Google Workspace, Social Media, Microsoft Teams, Zoom, Cisco WebEx, Google Meet
Marketing	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Google Workspace, Social Media, Microsoft Teams, Zoom, Cisco WebEx, Google Meet, YouTube, TikTok
Accounting	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Google Workspace, Microsoft Teams, Zoom, Cisco WebEx, Google Meet
Engineering	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Google Workspace, Microsoft Teams, Zoom, Cisco WebEx, Google Meet
System Admin	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Salesforce, Google Workspace, Social Media, Microsoft Teams, Zoom, Cisco WebEx, Google Meet, Netflix, Prime Video, Hulu, YouTube, TikTok, HBO Max, Disney+, AppleTV
User	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Salesforce, Google Workspace, Social Media, Microsoft Teams, Zoom, Cisco WebEx, Google Meet, YouTube, TikTok,
Super User	HTTP, HTTPS, DNS, SMTP, IMAP, POP3, Exchange, FTP, Office 365, Salesforce, Google Workspace, Social Media, Microsoft Teams, Zoom, Cisco WebEx, Google Meet, Netflix, Prime Video, Hulu, YouTube, TikTok, HBO Max, Disney+, AppleTV
Custom	As defined

Table 5 – Role and Target Users, Devices, and Applications Access Control Policy

[R21] The test **MUST** verify that the ZT implementation allows associating one or more policies with a Subject or Target Users, Devices, and Applications.

9.2.3.1 Scoring Penalty

The scoring penalty for section 9.2.3 is 25%.

9.2.4 Role and Capability Delegation

Test Objective: The ability of a ZT implementation to Inherit, Delegate or Indirectly Delegate Roles and capabilities to other Subject Users, Devices, and Applications is to be verified.

Test Process: A Subject User is defined with a Role and capabilities. The Role and capabilities of the Subject User are then Inherited by another Subject User, Delegated to another Subject User, and Indirectly Delegated to a Subject User. See section 8 for the list of defined policies that can be delegated.

[R22] The test **MUST** verify that the ZT implementation allows Policies to be inherited through Delegation or Indirect Delegation.

9.2.4.1 Scoring Penalty

The scoring penalty for section 9.2.4 is 15%.

9.3 Change Control

Test Objective: The system needs to track, retain, and report changes to policies and rules. Subject and Target Users, Devices, and Applications should also be monitored, and, if possible, change management controls should be implemented. These items fall under compliance process controls for change management, onboard and off-board, segregation of duties, and access control.

Change Control functionality and capabilities include support for each of the following:

- Roll-Back
- Revision History

Test Process: To test this, a policy is changed, and the test verifies that there is a log entry when the policy is changed. In addition, the test verifies that the policy version is automatically updated. The test also verifies that a policy can be rolled back to a previous version.

[R23] The test **MUST** verify that the ZT implementation supports change control.

9.3.1 Scoring Penalty

The scoring penalty for section 9.3 is 15%.

9.3.2 Policy Versioning

Test Objective: The ZT implementation should provide the ability to secure Policies through versioning and other methods.

Test Process: To test this, a policy is changed, and the test verifies that there is a log entry when the policy is changed. In addition, the test verifies that the policy version is automatically updated. The test also verifies that a policy can be rolled back to a previous version.

[R24] The test **MUST** verify that the ZT implementation secures Policies to eliminate the capability of tampering with them.

9.3.2.1 Scoring Penalty

The scoring penalty for section 9.3.2 is 25%.

10 Reporting Capabilities

Logging, alerting, and reporting are critical functions that inform the security posture and facilitate incident response actions. Reporting capabilities will be assessed to determine the ability of the ZT implementation to support these requirements.

10.1 Logs – Incident Response

Test Objective: All ZT implementations will be tested to determine if they retain log and event data to support the incident response process.

Test Process: Actions that cause the below events are performed and the results are captured.

Standardized logging and reporting formats, which facilitate the fast and accurate consumption of presented data, are imperative for administrators to validate conviction accuracy. The ZT implementation should allow easy generation and exportation of reports, logs, and alerts into industry-standard formats to support incident response. (Aspects like log time normalization, log file maintenance options, and forensic traffic capture will also be factored in the assessment.)

Editor Note 5: Comments on what information must be included in logs are requested.

[R25] The log Event **MUST** be tamper-proof

Tamper-proof in the context of this document is defined as per MEF 118 [5] to be a process which makes alterations to the data difficult (hard to perform), costly (expensive to perform), or both.

[R26] An audit Event **SHOULD** be encrypted with a security strength of at least 256 bits

Security strength in the context of this document is defined per MEF 118 [5] as a number associated with the amount of work, i.e., the number of operations, that is required to break a cryptographic algorithm or system. Note, the security strength is typically specified in bits.

Each Session is typically continuously monitored because either Subject or Target User, Device, or Application may have Risk calculation data from the Policy Information Point, or the Risk level determined by Risk-Awareness to be sufficiently high to Allow but not sufficiently high to Block the Session. Note that this monitoring is specific to this Session using the Continuous Monitoring techniques defined in MEF 118 [5].

The ZT implementation is expected to collect and store information about events, including the following:

- Administrator Login/Logout
- Successful Authentication
- Unsuccessful Authentication

- Successful Identify
- Unsuccessful Identify
- The Policy which was applied
- Who/What triggered the Policy Action
- Policy Changes
- Policy Deployment
- Policy Violations

[R27] The test MUST verify that a ZT implementation collects and stores information about the events in section 10.1.

10.1.1 Scoring Penalty

The scoring penalty for section 10.1 is 50%.

10.2 Reports

Reporting functionality is critical to ascertaining the system's state and investigating incidents. The ZT implementation will be assessed to determine the reporting capabilities that the implementation supports.

10.2.1 Report Automation

Test Objective: Verify that as a part of an implementation for reporting, ZT implementations are expected to provide the capability to schedule and deliver automated reports.

Test Process: Automated reports are configured and it is verified that they are generated with the appropriate information in them at the scheduled time.

[R28] The test **MUST** verify that a ZT implementation supports the capability to schedule and deliver automated reports.

10.2.1.1 Scoring Penalty

The scoring penalty for section 10.2.1 is 5%.

11 Testing of MEF 118 Requirements

The focus of this section is to identify which requirements from MEF 118 [5] are tested using the test methodologies defined in sections 8, 9, and 10.

Requirements are either Mandatory, meaning that they must be tested as a part of the certification, Optional, meaning that they may be tested as a part of the certification, or Deferred, meaning that they will not be tested at this time. Service Providers are not the focus of this version of the certification test and therefore those requirements focused on Service Providers are Deferred.

MEF 118 Requirement	Testable (T), Non-Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this Document	Comments
R1	T	D		SP Requirement
D1	T	O	Needs Test Methodology	
R2	N			
R3	T	M	8.1.7, 9.2	
D2	T	M	8.1.7, 9.2	
R4	T	M	8.1.7, 9.2	
R5	N			
R6	T	D		SP Requirement
D3	T	D		SP Requirement
O1	T	D		SP Requirement
R7	N			
R8	N			
R9	T	D		SP Requirement
CR1	T	O	Needs Test Methodology	CR support for OAuth required
R10	T	M	Needs Test Methodology	CR support for OAuth required
R11	T	D		SP Requirement
R12	T	M	9.1.1	
R13	N			SP Requirement
R14	T	M		PKI requirement. Not included in testing.
D4	T	O		PKI requirement. Not included in testing.
R15	T	M		PKI requirement. Not included in testing.
R16	T	M		PKI requirement. Not included in testing.
R17	T	M		PKI requirement. Not included in testing.
R18	T	M		PKI requirement. Not included in testing.
R19	T	M		PKI requirement. Not included in testing.
R20	T	M		PKI requirement. Not included in testing.
D5	T	M		PKI requirement. Not included in testing.
R21	N			

MEF 118 Requirement	Testable (T), Non-Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this Document	Comments
R22	T	M		PKI requirement. Not included in testing.
D6	T	O		PKI requirement. Not included in testing.
R23	T	M		PKI requirement. Not included in testing.
R24	N			
R25	N			
R26	N			
R27	T		9.1.2	
R28	N			
R29	T	M	Needs Test Methodology	
R30	T	D		SP Requirement
R31	N			
R32	N			
R33	T	M	8.1, 8.2	
R34	T	D		SP Requirement
R35	N	D		SP Requirement
R36	?	M	Needs Test Methodology	
R37	T	M		Unique IDs are hidden
R38	T	D		SP Requirement
R39	N			
R40	T	M	Needs Test Methodology	
R41	T	M	Needs Test Methodology	
R42	T	M	Needs Test Methodology	
R43	T	M	Needs Test Methodology	
R44	T	M	Needs Test Methodology	
D7	T	O	Needs Test Methodology	
R45	N			

MEF 118 Requirement	Testable (T), Non-Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this Document	Comments
R46	T	M	8.3	While ZT Vendors uniquely identify apps While, these are verified using different methods as described in section 8
R47	T	M	8.3	While ZT Vendors uniquely identify apps While, these are verified using different methods as described in section 8
R48	T	M	8.3	While ZT Vendors uniquely identify apps While, these are verified using different methods as described in section 8
R49	T	D		SP Requirement
R50	N			
R51	T	M		This is based on Figure 7 in MEF 118. Different ZT Vendor implementations will work differently and not align with that figure.
R52	T	M	9.1.1	
R53	T	M		This is based on Figure 7 in MEF 118. Different ZT Vendor implementations will work differently and not align with that figure.
D8	T	O		This is based on Figure 7 in MEF 118. Different ZT Vendor implementations will work differently and not align with that figure.
R54	T	M		This is based on Figure 7 in MEF 118. Different ZT Vendor implementations will work differently and not align with that figure.

MEF 118 Requirement	Testable (T), Non-Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this Document	Comments
R55	T	M		This is based on Figure 7 in MEF 118. Different ZT Vendor implementations will work differently and not align with that figure.
R56	T	M	9.1.1	
R57	T	M	9.1.1, 10.1, 10.2, 10.3	
R58	N			
D9	T	O	8.12.3	
R59	T	M	8.12.3	
R60	T	M	8.12.3	
R61	T	M	9.2	
R62	T	M		It Cannot be addressed at the network level.
R63	T	M		It Cannot be addressed at the network level.
R64	T	M		It Cannot be addressed at the network level.
D10	T	M	9.2	
R65	T	M		Covered in section 7
R66	T	M	9.2	
R67	T	M	9.2	
R68	T	M	9.2	
R69	T	M	9.2	
R70	T	M	9.2	
R71	T	M	9.1.1	
R72	T	M	9.1.1	
R73	T	M	9.1.1	
R74	T	M	9.1.1	
R75	T	M	9.1.1	
R76	T	M	9.1.1	
R77	T	M		This test applies to end points and not the network.
R78	T	M	9.1.1	
R79	T	M	9.1.1	
R80	T	M	9.1.1	
R81	T	M	9.1.1	
R82	T	M	9.1.1	

MEF 118 Requirement	Testable (T), Non-Testable (N)	Mandatory (M), Deferred (D), or Optional (O)	Test Methodology from this Document	Comments
R83	T	M	9.1.1	
R84	T	M	9.1.1	
R85	T	M	9.1.1	
R86	T	M	9.1.1	
R87	T	M	9.1.1	
R88	T	M	9.1.1	
R89	T	M	9.1.1	
R90	T	M	9.1.1	
R93	T	M	10.1	
R94	T	M	10.1	
R95	T	D		SP Requirement
R96	T	D		SP Requirement
R97	T	D		SP Requirement
R98	T	D		SP Requirement
D13	T	D		SP Requirement
CR6	T	D		SP Requirement

Table 6 – MEF 118 Requirements

12 Rating Methodology

The method used to determine the rating for an SD-WAN Edge ZT Vendor solution or an SP SWVC solution under test use objective methods to provide a rating. Ratings use a 0-to-800 point scale. The point values for each rating are shown in Table 7.

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

Table 7 – Rating Point Values

Each session of testing begins with the allocation of 800 points per section. Points are deducted from the 800 points when a test does not perform as specified.

Section Number	Total Points	Penalty	Comments
8.12.1		100%	
8.12.2		100%	
8.12.3		25%	
8.12.4		50%	
8.12.5		50%	
8.12.6		50%	
	800		
9.1.1		100%	
9.1.2		100%	
9.1.3		100%	
9.2.1		100%	
9.2.2		50%	
9.2.3		25%	
9.2.4		15%	
9.3		15%	
9.3.2		25%	
	800		
10.1		50%	
10.2.1		5%	
	800		
Total Points			

Table 8 – Point Penalty Allocation per Section

As seen in Table 8, some areas of testing are considered “table stakes” for ZT implementation, and test results that indicate that the expected capabilities are not provided result in a significant penalty.

Other testing areas are considered “nice to have” functions, and a lower penalty is deducted if the test results are not as expected.

The penalty percentage is calculated and deducted from the total points for each section, and the total points associated with the section are determined. The overall rating is determined based on the total points shown in Table 7. A rating is provided for each section of the document and the overall rating is an average of the per section rating.

12.1 MEF Certification Pass/Fail Criteria

To allow for a MEF Certification a Pass/Fail criteria has been defined within this section. Scores are calculated as described below.

It is proposed that a minimum of 90% of the requirements from MEF 118 [5] shown in section 11 of this document as testable are required to pass in order for an ZT solution to be eligible for MEF Certification. Solutions that fail to meet these criteria may still be provided a rating but are not MEF certified.

13 References

[1] IETF RFC 1918, *Address Allocation for Private Internets*, by Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, February 1996

[2] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, by Scott Bradner, March 1997

[3] IETF RFC 8174, *Ambiguity of Uppercase vs. Lowercase in RFC 2119 Key Words*, by B Leiba, May 2017, Copyright © 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

[4] MEF W90.2, *SD-WAN Certification Phase 2*, August 2023

[5] MEF 118, *Zero Trust Framework for MEF Services*, October 2022

[6] MEF W162, *Security Service Edge Certification Test Cases and Requirements*, August 2023