



Draft Standard MEF 131 Draft (R1)

MEF Secure SD-WAN Certification Test Requirements Release 1

**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

© MEF Forum 2022. All Rights Reserved.

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.

This draft document represents MEF work in progress, has not achieved full MEF standardization and is subject to change. There are known unresolved issues that are likely to result in changes before this becomes a fully endorsed MEF Standard. The reader is strongly encouraged to review the Release Notes 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.

Implementation or use of specific MEF standards, specifications, or recommendations will be voluntary. This document is provided "as is" with no warranties whatsoever, express or implied, including without limitation, any warranties of merchantability, non-infringement, accuracy, completeness or fitness for any particular purpose. MEF and its members disclaim all liability, including liability for infringement of any proprietary rights, relating to use of information in this document.

Table of Contents

1	List of Contributing Members	1
2	Abstract	2
3	Release Notes	2
4	Terminology and Abbreviations	3
5	Compliance Levels	3
6	Testable Functions and Requirements	4
7	Certification Test Requirements.....	5
8	Requirements Coverage	9
9	SD-WAN Application Security Certification Test Cases Description.....	14
Appendix A SD-WAN Performance Certification Test Cases Description		55
A.1	Introduction	58

List of Figures

Figure 1 - Secure SD-WAN Certification Test Configuration (generic)	5
Figure 2 - Relation of MEF 88 requirements to MEF 131 test cases	7
Figure 3 - Test Case lifecycle overview	8

List of Tables

Table 3 - Test Scenario Template.....	6
Table 1 - Requirements in Relation to Test Cases	9
Table 2 - Test Cases with Related Requirements.....	12
Table 4 - IETF Benchmarking Methodology for Network Security Device Performance Requirements Coverage.....	59

1 List of Contributing Members

The following members of the MEF participated in the development of this Standard 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 Ballot is eligible to be included by opting in before the Letter Ballot is initiated. Note that it is the MEF member that is listed here (typically a company or organization), not their individual representatives.

2 Abstract

This document describes the MEF Secure SD-WAN certification test requirements to validate conformance with the Application Flow Security for SD-WAN Services (MEF 88) [3]. The Secure SD-WAN Certification Test Requirements standard is functional, and hence implementation-independent.

Each requirement in MEF 88 has been analyzed to determine the value and testability of verifying conformance. Requirements traceability has been maintained to ensure that each of the MEF 88 (and other MEF standards) requirements deemed valuable and testable are covered by one or more certification test requirements (specified in this standard), detailed test requirements (specified in the ACTP Test Plan), and the test case implementations (ACTP Test Suite).

As such, the document is an important aid to service providers to prepare for successful certification of their services and products to verify conformance with MEF 88 standard.

The Secure SD-WAN Certification Test Requirements are intended to accelerate MEF 88 standards and market adoption, to achieve a rich open ecosystem.

The Secure SD-WAN Certification Test Requirements Standard adopts the conventions and concepts introduced in the MEF 88 [3] and MEF 70.1 [2] standards.

3 Release Notes

This document is current as of May 2022. Further review and updates are expected before this is finalized as a MEF standard.

4 Terminology and Abbreviations

Terminology and abbreviations used in this document are defined in MEF 88 [3] Section 3 and are not repeated here. In many cases, the normative definitions to terms are found in other documents, which are referenced in MEF 88.

Conventions adopted in this document is consistent with those utilized in MEF 70.1 [2] and MEF 88 [3].

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 **Error! Reference source not found.**, RFC 8174 **Error! Reference source not found.**) when, and only when, they appear in all capitals, as shown here. All key words 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. Items that are **OPTIONAL** (contain the words **MAY** or **OPTIONAL**) are labeled as [Ox] for optional.

This document does not introduce new requirements. All requirements referenced in this document are from MEF 88 [1].

6 Testable Functions and Requirements

This document defines certification test requirements for verifying conformance with MEF 88 as defined by all its requirements that satisfy two criteria:

- **Valuable:** Verification of conformance with a MEF 88 requirement offers a tangible benefit to the service provider. For example, verifying conformance with a particular security function specified in MEF 88 provides service providers with the confidence that the security function behaves in a consistent manner across different vendor implementations.
- **Testable:** Verification of conformance with a MEF 88 requirement can be performed in a cost effective and consistent manner. For example, a requirement may be valuable, but if specialized hardware is required to verify a requirement in a cloud-based certification environment, it may be infeasible to include the requirement in this specification.

More importantly, not all functionality and requirements are testable. Many items are not thoroughly defined in MEF 88, are implementation-specific, or are not readily measurable.

- The Requirements Coverage section (Section 6) lists MEF 88 requirements as R### (where R### is the Requirement number specified in MEF 88).

7 Certification Test Requirements

This section specifies the functional (implementation-independent) requirements to validate conformance with MEF 88 requirements. Certification Test Requirements coverage is summarized in Table I.

A generic Secure SD-WAN certification test environment is illustrated in Figure TBD. Security functions are exercised by test patterns originating from and terminating with the Traffic Generator/Analyzer based on the Test Scenarios described below.

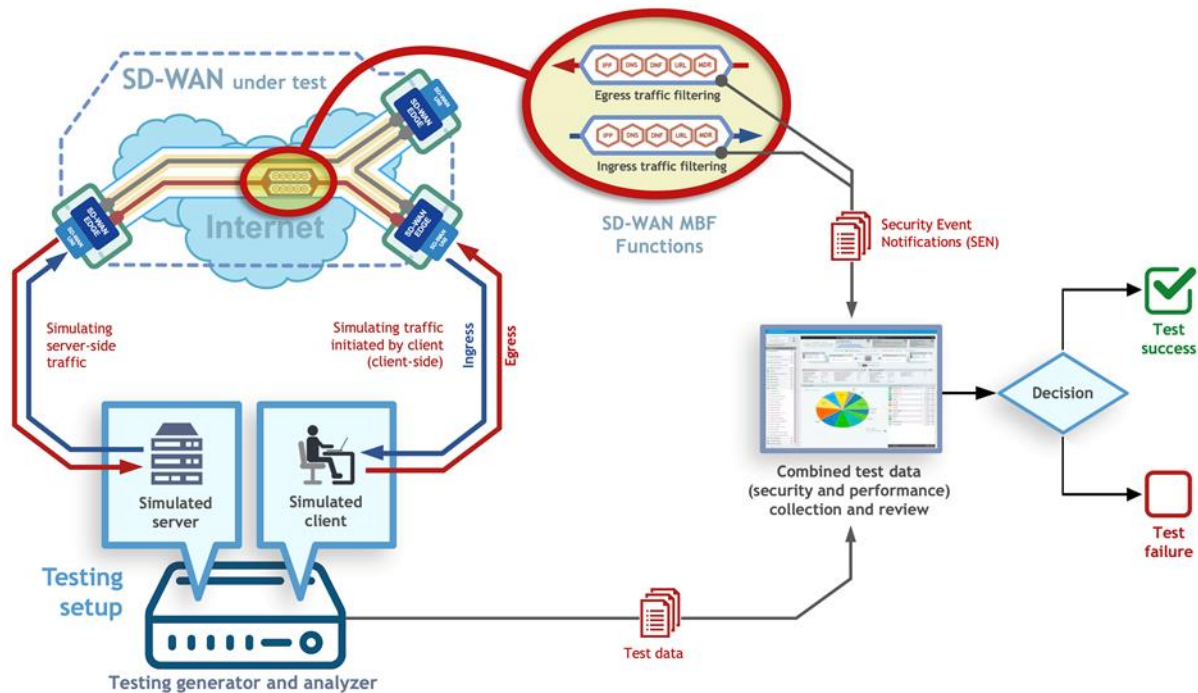


Figure 1 – Secure SD-WAN Certification Test Configuration (generic)

Test Scenarios

A Test Scenario consists of one or more test cases that are designed to verify conformance with one or more MEF 88 requirements. Test Scenarios are described using a common template, which is described in Table 2.

Table 1 – Test Scenario Template

Title	A brief overview of the Test Scenario.
Purpose of the test	Primary objective of the Test Scenario.
MEF 88 Requirement(s) Covered	The list of MEF 88 requirements that are covered by this Test Scenario.
Parameters	List of parameters, such as: URLs, domain names, IP addresses, credentials, etc. – everything which is required for the scenario.
Testing approach	How the test should be conducted: should it be performed with a user platform or an Application-Layer traffic generator/analyzer or both.
Testing process	List of steps to execute the test. For example, configuring client-initiated network traffic to two URLs; the first URL is allowlisted and the second URL is blocklisted. Then the traffic requests are sent using both URLs and verify the results.
Test success criteria	Information about what should happen to pass the test, according to the testing process. Success criteria are different for different scenarios. The expected outcome is explicitly specified for success and failure. For example, sending the client-initiated network traffic to two URLs; the first URL is allowlisted and the second URL is blocklisted. It should be possible to access the first one, and at the same time , it should not be possible to access the second one. In case of success with both steps i.e., accessing the first URL and not accessing the second URL, then the test is passed.

Types of Tests

As presented in Section 6, each Test Case can cover one or more MEF 88 Requirements. This is possible due to the fact that each Test Case can have one or more Tests. There is no mandatory direct relationship between the number of Tests and related Requirements as one Test can cover more than one MEF 88 Requirement. As illustrated with the example in Figure 2, there is a sample test case comprised of three tests and covering MEF 88 Requirements 5, 6 and 7.

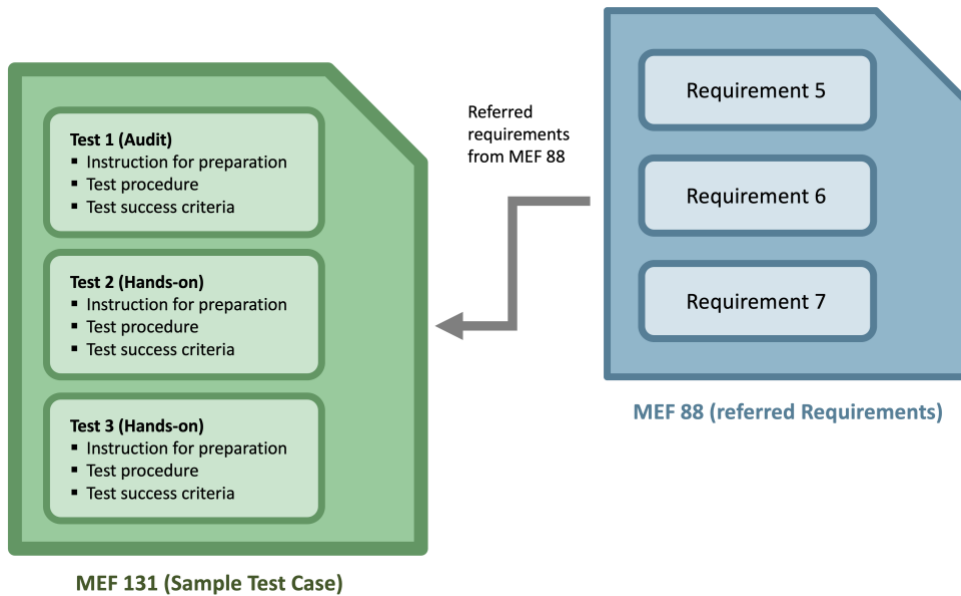


Figure 2 – Relation of MEF 88 requirements to MEF 131 test cases

We distinguish two types of Tests:

1. Audit
2. Hands-on

An **Audit type of test** is used when it is just enough to witness the existence of some functionality in the system (provided in UI or through a machine-friendly interface) or to have a proof (or declaration) from the SD-WAN Service Provider that the examined functionality is in place.

Example 1: Checking if the Notification Event log (SEN) can be accessed in the SD-WAN administrative interface.

Example 2: Checking if the frequency of virus feed update is specified in the SP's SLA (e.g., the update happens every month).

A **Hands-On type of test** is used when the auditor is required to interact with the tested system. This means that the auditor could try to change the system's configuration, modify the network traffic rules, generate some traffic, or access some specific resources through SD-WAN according to the Test scenario.

It should be noted that both types of activities can be executed manually or automatically, dependent on the options made available by the Service Provider. For the same reason, in this document, we do not discuss technical details regarding how each Test should be implemented.

Test lifecycle

Typically, before executing a test, some preparation is required, such as accessing some functionality or configuring SD-WAN network traffic rules. The description of what should be prepared/configured is described in the common section “Preparation” within each Test Case.

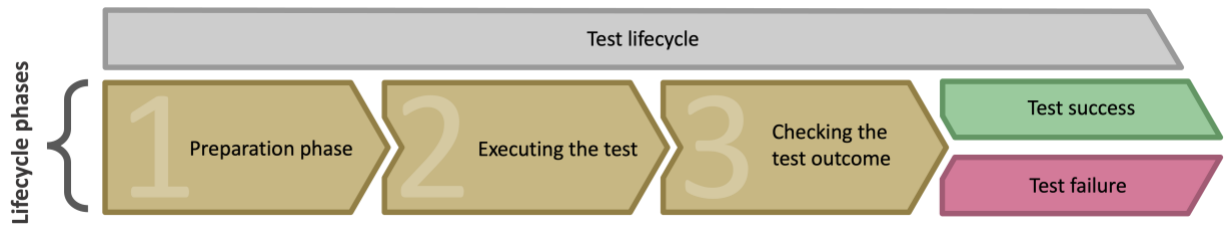


Figure 3 – Test Case lifecycle overview

8 Requirements Coverage

Each MEF 88 requirement was assessed to determine both the value and feasibility of developing a certification test requirement to verify conformance, as indicated in Table I below.

This section addresses each major functional area of MEF 88, and the certification test requirements to verify each MEF 88 requirement.

Traceability between each MEF 88 requirement, and its associated certification test requirements is listed in Table 2.

Table 2 – Requirements in Relation to Test Cases

MEF 88 Req.	Section	Testable	Related Test Cases
[R1]	[6]	Yes	[TC1]
[R2]	[6] -> [6.1]	Yes	[TC2]
[R3]	[6] -> [6.1]	Yes	[TC2]
[R4]	[6] -> [6.1]	Yes	[TC2]
[R5]	[7] -> [7.1] -> [7.1.1]	Yes	[TC3]
[R6]	[7] -> [7.1] -> [7.1.1]	Yes	[TC3]
[R7]	[7] -> [7.1] -> [7.1.1]	Yes	[TC3]
[R8]	[7] -> [7.1] -> [7.1.1]	Yes	[TC4]
[R9]	[7] -> [7.1] -> [7.1.1]	Yes	[TC5]
[R10]	[7] -> [7.1] -> [7.1.1]	Yes	[TC6]
[R11]	[7] -> [7.1] -> [7.1.2]	Yes	[TC7]
[R12]	[7] -> [7.1] -> [7.1.2]	Yes	[TC7]
[R13]	[7] -> [7.1] -> [7.1.3]	Yes	[TC8]
[R14]	[7] -> [7.1] -> [7.1.3]	Yes	[TC8]
[R15]	[7] -> [7.1] -> [7.1.4]	Yes	[TC9]
[R16]	[7] -> [7.2]	Yes	[TC20], [TC21], [TC19], [TC14], [TC23], [TC22], [TC18]
[R17]	[7] -> [7.2]	Yes	[TC10]
[R18]	[7] -> [7.2]	Yes	[TC11]
[R19]	[7] -> [7.2]	Yes	[TC11]
[R20]	[7] -> [7.2]	Yes	[TC11]
[R21]	[7] -> [7.2]	Yes	[TC12]
[R22]	[8]	Yes	[TC13]
[R23]	[8]	Yes	[TC13]
[R24]	[8]	Yes	[TC13]
[R25]	[8]	Yes	[TC13]
[R26]	[8]	Yes	[TC13]
[R27]	[8]	Yes	[TC13]
[R28]	[8]	Yes	[TC13]

[R29]	[8]	Yes	[TC13]
[R30]	[8]	Yes	[TC14]
[R31]	[8]	Yes	[TC15]
[R32]	[8]	Yes	[TC14]
[R33]	[8]	Yes	[TC14]
[R34]	[8]	Yes	[TC14]
[R35]	[8]	Yes	[TC16]
[R36]	[8]	Yes	[TC16]
[R37]	[8]	Yes	[TC17]
[R38]	[8]	Yes	[TC17]
[R39]	[8]	Yes	[TC17]
[R40]	[8] -> [8.1]	Yes	[TC17]
[R41]	[8] -> [8.1]	Yes	[TC18]
[R42]	[8] -> [8.1]	Yes	[TC18]
[R43]	[8] -> [8.1]	Yes	[TC17]
[R44]	[8] -> [8.1]	Yes	[TC17]
[R45]	[8] -> [8.1]	Yes	[TC17]
[R46]	[8] -> [8.1]	Yes	[TC18]
[R47]	[8] -> [8.1]	Yes	[TC18]
[R48]	[8] -> [8.1]	Yes	[TC18]
[R49]	[9] -> [9.1]	Yes	[TC19]
[R50]	[9] -> [9.1]	Yes	[TC19]
[R51]	[9] -> [9.1]	Yes	[TC19]
[R52]	[9] -> [9.1]	Yes	[TC19]
[R53]	[9] -> [9.2]	Yes	[TC20]
[R54]	[9] -> [9.2]	Yes	[TC20]
[R55]	[9] -> [9.2]	Yes	[TC20]
[R56]	[9] -> [9.2]	Yes	[TC20]
[R57]	[9] -> [9.2]	Yes	[TC20]
[R58]	[9] -> [9.3]	Yes	[TC21]
[R59]	[9] -> [9.3]	Yes	[TC21]
[R60]	[9] -> [9.3]	Yes	[TC21]
[R61]	[9] -> [9.3]	Yes	[TC21]
[R62]	[9] -> [9.3]	Yes	[TC21]
[R63]	[9] -> [9.3]	Yes	[TC21]
[R64]	[9] -> [9.3]	Yes	[TC21]
[R65]	[9] -> [9.4]	Yes	[TC22]
[R66]	[9] -> [9.4]	Yes	[TC22]
[R67]	[9] -> [9.4]	Yes	[TC22]
[R68]	[9] -> [9.4]	Yes	[TC22]
[R69]	[9] -> [9.4]	Yes	[TC22]
[R70]	[9] -> [9.4]	Yes	[TC22]

[R71]	[9] -> [9.4]	Yes	[TC22]
[R72]	[9] -> [9.5]	Yes	[TC23]
[R73]	[9] -> [9.5]	Yes	[TC23]
[R74]	[9] -> [9.5]	Yes	[TC23]
[R75]	[9] -> [9.5]	Yes	[TC23]
[R76]	[9] -> [9.5]	Yes	[TC23]
[R77]	[9] -> [9.5]	Yes	[TC23]

Table 3 – Test Cases with Related Requirements

Test No.	Test Name	Related requirements	Notes
1	[TC1] Reviewing performance notification clauses in SD-WAN notification mechanisms	[R1]	
2	[TC2] Reviewing Security Policy Identifier parameters	[R2], [R3], [R4]	
3	[TC3] Reviewing Security Policy Block List basic management	[R5], [R6], [R7]	
4	[TC4] Reviewing Security Policy Block List (entries locked by Service Provider)	[R8]	
5	[TC5] Reviewing security threat database update time frame	[R9]	
6	[TC6] Reviewing change request clauses in SD-WAN notification mechanisms	[R10]	
7	[TC7] Reviewing Security Policy Allow List basic management	[R11], [R12]	
8	[TC8] Reviewing Security Policy Quarantine List basic management	[R13], [R14]	
9	[TC9] Reviewing requirements pertaining to all of the Lists	[R15]	
10	[TC10] Reviewing SEN storage mechanisms	[R17]	
11	[TC11] Reviewing SEN report fields	[R18], [R19], [R20]	
12	[TC12] Reviewing SEN reporting mechanisms	[R21]	
13	[TC13] Reviewing the MBF basic maintenance	[R22], [R23], [R24], [R25], [R26], [R27], [R28], [R29]	
14	[TC14] Reviewing the processing of Application Flow by MBF	[R16], [R30], [R32], [R33], [R34]	
15	[TC15] Reviewing decryption of Application Flow by MBF	[R31]	
16	[TC16] Reviewing if the MBF support for TLS 1.2	[R35], [R36]	
17	[TC17] Reviewing the decryption of the TLS traffic by MBF	[R37], [R38], [R39], [R40], [R43], [R44], [R45]	
18	[TC18] Reviewing if MBF verifies the validity of the targeted server certificate	[R16], [R41], [R42], [R46], [R47], [R48]	
19	[TC19] Reviewing the IPPF filtering functionality	[R16], [R49], [R50], [R51], [R52]	
20	[TC20] Reviewing the DNS filtering functionality	[R16], [R53], [R54], [R55], [R56], [R57]	
21	[TC21] Reviewing the Domain Name Filtering functionality	[R16], [R58], [R59], [R60], [R61], [R62], [R63], [R64]	

22	[TC22] Reviewing the URL Filtering functionality	[R16], [R65], [R66], [R67], [R68], [R69], [R70], [R71]	
23	[TC23] Reviewing the Malware Detection and Removal functionality	[R16], [R72], [R73], [R74], [R75], [R76], [R77]	

9 SD-WAN Application Security Certification Test Cases Description

This section describes the test cases based on MEF 88.

Test case #1	Verify basic SD-WAN notification mechanisms
Purpose:	Verify the Service Provider informs the Subscriber of any expected impact to the SD-WAN service performance
Related requirement(s):	<i>[R1] When a Security Policy is in force for a given Application Flow, the Service Provider MUST inform the Subscriber of any expected impact to the SD-WAN service performance.</i>
Parameters:	Access to any means or method for Service Provider to inform the Subscriber about the basic SD-WAN configuration (could be SLA, special section in the SD-WAN administrative functionality, or API request for this data to SD-WAN controller) hereinafter called “SD-WAN notification mechanisms”
Testing approach:	Manual audit of the SD-WAN notification mechanisms
Testing process:	Test 1 (audit): Inspect the Subscriber’s SD-WAN notification mechanisms and verify that SP provides the Subscriber with information about any expected impact of enabled security policy to the SD-WAN service performance.
Test success criteria:	Test 1 (audit): Auditor can confirm that the SD-WAN notification mechanisms provide the information about any expected impact of enabled security policy to the SD-WAN service performance.

Test case #2	Verify Security Policy Identifiers
Purpose:	Verify Security Policy identifier requirements
Related requirement(s):	<p><i>[R2] The Security Policy Identifier MUST be an Identifier String.</i></p> <p><i>[R3] Each Security Policy Identifier MUST be unique among all Security Policies for a given SWVC.</i></p> <p><i>[R4] The value of the Security Policy Identifier MUST NOT be none.</i></p>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Review the selected Security Policy and ensure that its Identifier is an Identifier String <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Try to create a new Security Policy with the same Identifier as in any existing Policy <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Try to create a new Security Policy with an empty Identifier
Test success criteria:	<p>Test1 (audit):</p> <ul style="list-style-type: none"> - The Security Policy Identifier is an Identifier String <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - It is not possible to create a new Security Policy with the same Identifier String as in any existing Policy <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - It is not possible to create a new Security Policy with an empty Identifier String

Test case #3	Verify Security Policy Block List management
Purpose:	Verify Security Policy block list management requirements
Related requirement(s):	<p><i>[R5] For each Security Function, the Service Provider MUST maintain a list of match criteria entries in the Block List.</i></p> <p><i>[R6] For each Security Function, the Service Provider MUST allow the Subscriber to add match criteria entries to the Block List.</i></p> <p><i>[R7] For each Security Function, the Service Provider MUST allow the Subscriber to remove a match criteria entry on the Block List that was added by one of the following methods:</i></p> <ul style="list-style-type: none"> <i>- Specified explicitly by the Subscriber</i> <i>- Specified by the Service Provider to conform to a category specified by the Subscriber</i>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Validate if the Service Provider maintains a list of match criteria entries in the Block List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to add match criteria entries to the Block List. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to remove a match criteria entry on the Block List that was added by one of the following methods: - Specified explicitly by the Subscriber - Specified by the Service Provider to conform to a category specified by the Subscriber
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - For each security function, the Service Provider maintains a list of match criteria entries in the Block List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - For each Security Function, the Service Provider allows the Subscriber to add match criteria entries to the Block List.

	Test 3 (audit): - For each Security Function, the Service Provider allows the Subscriber to remove match criteria entries (created by both methods) from the Block List
--	---

Test case #4	Verify Security Policy Block List (entries locked by Service Provider)
Purpose:	Verify Security Policy Block List locking requirements
Related requirement(s):	<i>[R8] For each Security Function, the Service Provider MUST NOT allow the Subscriber to remove a match criteria entry from the Block List that the Service Provider specified due to a security threat.</i>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy <p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - Try to remove a match criteria entry from the Block List that the Service Provider specified due to a security threat.
Test success criteria:	<p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - It is not possible to remove a match criteria entry from the Block List that the Service Provider specified due to a security threat.

Test case #5	Verify security threat database update time frame
Purpose:	Verify the Service Provider provides the Subscriber with the time frame used to update the security threat database.
Related requirement(s):	<i>[R9] For each Security Function, the Service Provider MUST provide to the Subscriber the time frame used to update the security threat database.</i>
Parameters:	Access to any means or method for Service Provider to inform the Subscriber about the basic SD-WAN configuration (could be SLA, special section in the SD-WAN administrative functionality, or API request for this data to SD-WAN controller) hereinafter called “SD-WAN notification mechanisms”
Testing approach:	Manual audit of the SD-WAN notification mechanisms
Testing process:	Test 1 (audit): - Examine the SD-WAN notification mechanisms and ensure that there is(are) an appropriate clause(s) in place. The clause should specify the time frame that the Service Provider provides the Subscriber with for regular updates of the security threat database.
Test success criteria:	Test 1 (audit): - The SD-WAN notification mechanisms specifies the time frame for regular updates of the security threat database.

Test case #6	Verify change request clauses in SD-WAN notification mechanisms
Purpose:	Verify that for each Security Function, the Service Provider provides a documented process to allow the Subscriber to request a change to an entry on the Block List that the Service Provider specified due to a security threat.
Related requirement(s):	<i>[R10] For each Security Function, the Service Provider MUST provide a documented process to allow the Subscriber to request a change to an entry on the Block List that the Service Provider specified due to a security threat.</i>
Parameters:	Access to any means or method for the Service Provider to inform the Subscriber about the basic SD-WAN configuration (could be SLA, special section in the SD-WAN administrative functionality, or API request for this data to SD-WAN controller) hereinafter called “SD-WAN notification mechanisms”
Testing approach:	Manual audit of the SD-WAN notification mechanisms
Testing process:	Test 1 (audit): <ul style="list-style-type: none"> - Examine the SD-WAN notification mechanisms and ensure that there is(are) an appropriate clause(s) in place. The clause should specify that for each Security Function, the Service Provider provides a documented process to allow the Subscriber to request a change to an entry on the Block List that the Service Provider specified due to a security threat.
Test success criteria:	Test 1 (audit): <ul style="list-style-type: none"> - For each security function, the Service Provider provides a documented process to allow the Subscriber to request a change to an entry on the Block List that the Service Provider specified due to a security threat.

Test case #7	Verify Security Policy Allow List management
Purpose:	Verify Security Policies Allow List management requirements
Related requirement(s):	<p><i>[R11] For each Security Function, the Service Provider MUST maintain a list of match criteria entries in the Allow List.</i></p> <p><i>[R12] For each Security Function, the Service Provider MUST allow the Subscriber to add or remove match criteria entries in the Allow List.</i></p>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Validate if the Service Provider maintains a list of match criteria entries in the Allow List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to add match criteria entries to the Allow List.y <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to remove match criteria entries from the Allow List.
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - The Service Provider maintains a list of match criteria entries in the Allow List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - For each Security Function, Subscriber may add match criteria entries to the Allow List. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - For each Security Function, the Subscriber may remove match criteria entries from the Allow List.
Test case #8	Verify Security Policy Quarantine List management
Purpose:	Verify Security Policy Quarantine List basic management requirements
Related requirement(s):	<i>[R13] For each Security Function, the Service Provider MUST maintain a list of match criteria entries in the Quarantine List.</i>

	<p><i>[R14] For each Security Function, the Service Provider MUST allow the Subscriber to do each of the following:</i></p> <ul style="list-style-type: none"> - add match criteria entries to the Quarantine List - remove match criteria entries from the Quarantine List
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Validate if the Service Provider maintains a list of match criteria entries in the Quarantine List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to add match criteria entries to the Quarantine List. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - Validate if for each Security Function, the Service Provider allows the Subscriber to remove match criteria entries from the Quarantine List.
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - The Service Provider maintains a list of match criteria entries in the Quarantine List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> -For each Security Function, the Subscriber may add match criteria entries to the Quarantine List. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - For each Security Function, the Subscriber may remove match criteria entries from the Quarantine List.

Test case #9	Verify match criteria appears on only one list
Purpose:	Verify match criteria entry may appear on one list maximum
Related requirement(s):	<i>[R15] For each Security Function, the Service Provider MUST ensure that each match criteria entry is on at most one list.</i>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Access configuration of a sample Security Policy (policy 1) <p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - Take any match criteria (e.g. matching URL(s) from the Block List) and make the exact copy of the same criteria in the Allow List and/or Quarantine List). - Save and try to enable the modified Security Policy (policy 1) <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Open another Security Policy (policy 2) - Take any match criteria (e.g. matching URL(s) from the Block List of policy 1 and make the exact copy of the same criteria in Allow List and/or Quarantine List of policy 2). - Save and try to enable the modified Security Policy (policy 2)
Test success criteria:	<p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - It should not be possible to run the modified policy when the same matching criteria are on two lists in the same Security Policy (policy 1). <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - It should not be possible to enable the modified policy when the same matching criteria are on two lists in two Security Policies (policy 1 and policy 2). - An error message should be returned to the Subscriber

Test case #10	Verify SEN storage mechanisms
Purpose:	Verify Service Provider stores each Security Event Notification (SEN) in a secure repository for future reference and security auditing purposes.
Related requirement(s):	<i>[R17] The Service Provider MUST store each SEN in a secure repository for future reference and security auditing purposes.</i>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Examine SEN storage functionality and ensure that the Service Provider stores each SEN in a secure repository for future reference and security auditing purposes.
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Service Provider stores each SEN in a secure repository for future reference and security auditing purposes.

Test case #11	Verify SEN report fields
Purpose:	Verify Security Event Notification field requirements
Related requirement(s):	<p><i>[R18] A SEN MUST include the items listed in Table 2:</i></p> <p><i>ITEM: Issuer</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Examples: Service Provider Name, Security Vendor Name, etc.</i></p> <p><i>ITEM: Timestamp of IOC</i> <i>VALUE: date-time</i> <i>COMMENTS: RFC 3339 [8] Example: UTC</i></p> <p><i>ITEM: SEN ID</i> <i>VALUE: UUID</i> <i>COMMENTS: RFC 4122 [13] Universally Unique Identifier</i></p> <p><i>ITEM: Zone ID</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: MEF 70.1 [2]</i></p> <p><i>ITEM: Source IP address</i> <i>VALUE: Human readable, IPv4 dotted decimal, IPv6 hexadecimal strings</i> <i>COMMENTS: IANA Number Resources [28]</i></p> <p><i>ITEM: SD-WAN UNI ID</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: MEF 70.1 [2]</i></p> <p><i>ITEM: IOC Type</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Examples: CVE [37], STIX [40], CWE [35], CAPEC [39], ATT&CK [38], RFC 7970 [22].</i></p> <p><i>ITEM: IOC Information ID</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Identifies the IOC based on type</i></p> <p><i>ITEM: IOC Source</i> <i>VALUE: URL for the IOC type</i> <i>COMMENTS: CVE [37]</i></p> <p><i>ITEM: Type of Compromise</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Examples: known vulnerability, breach, data leakage, abuse of resources, jacking, where to find more information on the breach.</i></p> <p><i>ITEM: Compromise details</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Examples: Username, Source/Destination IP address, Source Media Access Control (MAC) address, neutralized URL, neutralized domain, Malware, Source/Destination port number, anomalous behavior.</i></p>

	<p><i>ITEM: Action Taken</i> <i>VALUE: UTF-8 [10] String</i> <i>COMMENTS: Examples: informational, quarantined or Blocked, Malware removed</i></p> <p><i>[R19] Any domain name or URL in a SEN MUST be neutralized.</i> <i>[D1] The method for neutralizing the domain name or URL in a SEN SHOULD use square brackets around each period.</i></p> <p><i>[R20] The Service Provider MUST support UTC for the timestamp format.</i></p>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Examine SEN storage functionality and ensure that each SEN has all the fields specified by MEF 88. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Examine SEN fields and ensure that any domain name or URL in SEN is neutralized (as per [R19]). <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - Examine SEN fields and ensure that the Service Provider supports UTC for the timestamp format.
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Each stored SEN has all the fields specified by [R18] <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Any domain name or URL in SEN is neutralized, per [R19] <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - The Service Provider supports UTC for the timestamp format for SENs.

Test case #12	Verify SEN recipient list
Purpose:	Verify SEN has configured a recipient list, which is agreed between the Service Provider and the Subscriber.
Related requirement(s):	<i>[R21] A SEN MUST have a recipient list, which is agreed between the Service Provider and the Subscriber.</i>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Examine the SEN configuration functionality and ensure that it has configured a recipient list, which is agreed between the Service Provider and the Subscriber.
Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Service Provider maintain a SEN recipient list agreed to between the Service Provider and the Subscriber.

Test case #13	Verify MBF List Management
Purpose:	Verify Middle Box Function (MBF) list management requirements
Related requirement(s):	<p><i>[R22] Based on agreement with the Subscriber, the Service Provider MUST maintain a list of match criteria entries in the MBF Supported List.</i></p> <p><i>[R23] Based on agreement with the Subscriber, the Service Provider MUST maintain a list of match criteria entries in the MBF Unsupported List.</i></p> <p><i>[R24] The Service Provider MUST ensure that a match criteria entry on the MBF Supported List cannot also appear on the MBF Unsupported List.</i></p> <p><i>[R25] When MBF is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the MBF Block List and the MBF Allow List.</i></p> <p><i>[R26] The Service Provider MUST ensure that each match criteria entry on the MBF Supported List is also on either the MBF Allow List or the MBF Block List.</i></p> <p><i>[R27] The Service Provider MUST ensure that each match criteria entry on the MBF Unsupported List is also on either the MBF Allow List or the MBF Block List.</i></p> <p><i>[R28] The Service Provider MUST ensure that each match criteria entry on the MBF Allow List is also on either the MBF Supported List or the MBF Unsupported List.</i></p> <p><i>[R29] The Service Provider MUST ensure that each match criteria entry on the MBF Block List is also on either the MBF Supported List or the MBF Unsupported List.</i></p>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual audit
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that, based on agreement with the Subscriber, the Service Provider maintains a list of match criteria entries in the MBF Supported List. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that, based on agreement with the Subscriber, the Service Provider maintains a list of match criteria entries in the MBF Unsupported List. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that a match criteria entry on the MBF Supported List cannot also appear on the MBF Unsupported List.

	<p>Test 4 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that when MBF is Enabled for a given Application Flow, the Service Provider meets the mandatory requirements specified in Section 7.1 of MEF 88 document relating to the MBF Block List and the MBF Allow List. <p>Test 5 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that each match criteria entry on the MBF Supported List is also on either the MBF Allow List or the MBF Block List. <p>Test 6 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that each match criteria entry on the MBF Unsupported List is also on either the MBF Allow List or the MBF Block List. <p>Test 7 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that each match criteria entry on the MBF Allow List is also on either the MBF Supported List or the MBF Unsupported List. <p>Test 8 (audit):</p> <ul style="list-style-type: none"> - Examine the MBF configuration functionality and ensure that each match criteria entry on the MBF Block List is also on either the MBF Supported List or the MBF Unsupported List.
<p>Test success criteria:</p>	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Service Provider maintains a list of match criteria entries in the MBF Supported List, agreed to by the Subscriber. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - Service Provider maintains a list of match criteria entries in the MBF Unsupported List, agreed to by the Subscriber. <p>Test 3 (audit):</p> <ul style="list-style-type: none"> - A match criteria entry on the MBF Supported List cannot also appear on the MBF Unsupported List. <p>Test 4 (audit):</p> <ul style="list-style-type: none"> - When MBF is Enabled for a given Application Flow, the Service Provider satisfies [R25], [R26], [R27], [R28], and [R29] relating to the MBF Block List and the MBF Allow List. <p>Test 5 (audit):</p> <ul style="list-style-type: none"> - Each match criteria entry on the MBF Supported List is also on either the MBF Allow List or the MBF Block List. <p>Test 6 (audit):</p> <ul style="list-style-type: none"> - Each match criteria entry on the MBF Unsupported List is also on either the MBF Allow List or the MBF Block List.

	<p>Test 7 (audit):</p> <ul style="list-style-type: none">- Each match criteria entry on the MBF Allow List is also on either the MBF Supported List or the MBF Unsupported List. <p>Test 8 (audit):</p> <ul style="list-style-type: none">- Each match criteria entry on the MBF Block List is also on either the MBF Supported List or the MBF Unsupported List.
--	---

Test case #14	Verify MBF Application Flow processing
Purpose:	Verify MBF is correctly processing security rules for the given Application Flow
Related requirement(s):	<p><i>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</i></p> <p><i>[R30] When MBF is Enabled for a given Application Flow, the subset of the Application Flow that matches a match criteria entry on the MBF Block List MUST be Blocked.</i></p> <p><i>[R32] When MBF is Enabled for a given Application Flow, the subset of the Application Flow that matches a match criteria entry on the MBF Allow List and on the MBF Unsupported List MUST be passed through the MBF without change.</i></p> <p><i>[R33] When MBF is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the MBF lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Pass the subset of the Application Flow through the MBF without change <p><i>[R34] When MBF is Enabled for a given Application Flow, the MBF Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the MBF lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Pass the subset of the Application Flow through the MBF without change
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Simulated test web resource accessible over TLS (website 1)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule by adding the matching criteria of website 1 (e.g., URL, IP address, specific TLS version, etc.) to the MBF Block List <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Examine the SD-WAN configuration functionality and ensure that the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the MBF lists: - Block the subset of the Application Flow - Pass the subset of the Application Flow through the MBF without change <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Establish a connection to the simulated web resource (website 1) <p>Test 3 (hands-on):</p>

	<ul style="list-style-type: none"> - Create and enable a new policy rule by adding the matching criteria of website 1 (e.g., URL, IP address, specific TLS version, etc.) to a) the MBF Allow List and b) the MBF Unsupported List - Establish a connection to the simulated web resource (website 1) - Examine the TLS certificate and confirm its issuer
Test success criteria:	<p>Test 1 (audit): When MBF is Enabled for Application Flows that do not match a match criteria entry on any of the MBF lists the following actions are taken:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Pass the subset of the Application Flow through the MBF without change <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Access to website 1 is blocked - SEN is triggered <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Website 1 is accessed - The original certificate provided by the website is in use (not the one provided by MBF)

Test case #15	Verify MBF Application Flow decryption
Purpose:	Verify that when MBF is Enabled, Application Flows that match the match criteria entry on the MBF Allow List and on the MBF Supported List are decrypted.
Related requirement(s):	<i>[R31] When MBF is Enabled for a given Application Flow, the subset of the Application Flow that matches a match criteria entry on the MBF Allow List and on the MBF Supported List MUST be decrypted.</i>
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated test web resource accessible over TLS (website 1) with known predefined TLS parameters (TLS version and cipher suites).
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule by adding the parameters of website 1 (e.g., URL, IP address, specific TLS version, etc.) to the MBF Allow List and MBF Supported list. <p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - Establish a connection to the simulated web resource (website 1) through the tested SD-WAN - Examine the TLS certificate and confirm its issuer
Test success criteria:	<p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - Website 1 is accessed - The Application Flow is successfully decrypted and re-encrypted by MBF - a client's trusted certificate should be in use

Test case #16	Verify MBF support for TLS 1.2
Purpose:	Verify MBF meets the mandatory requirements of TLS 1.2, per RFC 5246 and section 9.3 of RFC 8446 (Protocol Invariants).
Related requirement(s):	<p><i>[R35] The MBF MUST meet the mandatory requirements of TLS 1.2, per RFC 5246.</i></p> <p><i>[R36] The MBF MUST meet the mandatory requirements of section 9.3 of RFC 8446 (Protocol Invariants).</i></p>
Parameters:	Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Establish access to the SD-WAN diagnostic/administrative functionality, available to Subscriber <p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - Query the MBF diagnostic/administrative functionality (manually or automatically) and confirm if there is support for TLS 1.2 as per RFC 5246 <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Query the MBF diagnostic/administrative functionality (manually or automatically) and confirm if there is support for TLS Protocol Invariants as per section 9.3 of RFC 8446
Test success criteria:	<p>Test 1 (hands-on):</p> <ul style="list-style-type: none"> - The MBF diagnostic functionality returns information that TLS 1.2 is on the list of supported TLS versions <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - The MBF diagnostic/administrative functionality supports TLS Protocol Invariants as per section 9.3 of RFC 8446

Test case #17	Verify MBF decryption of TLS traffic
Purpose:	Verify that the TLS version and cipher suites are the same after re-encryption as in the original TLS
Related requirement(s):	<p><i>[R37] When MBF is Enabled for a given Application Flow, the MBF MUST NOT change the TLS protocol version for a TLS session as compared to the client request.</i></p> <p><i>[R38] When MBF is Enabled for a given Application Flow, the MBF MUST NOT choose a weaker cipher suite in the negotiation for a TLS session as compared to the TLS session without the MBF.</i></p> <p><i>[R39] An Application Flow decrypted by the MBF MUST NOT be exposed outside the Service Provider's Security Functions in an unencrypted form or in an encrypted form that offers a lower level of confidentiality and integrity than the originally encrypted Application Flow.</i></p> <p><i>[R40] The MBF MUST be capable of issuing a valid, signed certificate for each TLS session with a CA that is trusted by the Subscriber.</i></p> <p><i>[R43] Server certificates MUST be generated and regenerated with fresh, suitably random material per the requirements in FIPS-140-2 for which the MBF processes Application Flows.</i></p> <p><i>[R44] All replacement certificate properties, e.g., alternative server names, validity periods, and choices of cipher suites MUST NOT reduce the level of security functionality of the properties of the certificate being replaced.</i></p> <p><i>[R45] Where a CA is operated in support of the TLS inspection within the MBF, it MUST clearly identify itself within the visible issuer properties (as defined in Section 4.1.2.4 of RFC 5280) of the certificates that it signs for reasons of transparency, so that the Subscriber can identify when MBF is in the path versus when they are connecting directly to the originating server.</i></p> <p><i>[D2] Any TLS based interception being performed by an MBF as part of a managed service SHOULD use a Public Key Infrastructure (PKI) hierarchy that is rooted in a CA that is operated in line with the CA/Browser Forum baseline requirements where certificates are securely created, used, revoked and destroyed.</i></p> <p><i>[D3] Where possible, CAs SHOULD log any certificates that they issue using the standardized Certificate Transparency (CT) security standard, see RFC 6962.</i></p>
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber - Simulated test web resource accessible over TLS (website 1) with known predefined TLS parameters (TLS version and cipher suites).
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically)

	<ul style="list-style-type: none"> - Create and enable a new policy rule by adding the parameters of website 1 to the MBF Allow List - Establish a connection to the simulated web resource through the tested SD-WAN <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - It should be confirmed that an Application Flow decrypted by the MBF is not exposed outside the Service Provider's Security Functions in an unencrypted form or in an encrypted form that offers a lower level of confidentiality and integrity than the originally encrypted Application Flow. <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - Examine the TLS certificate offered by MBF. Check if it is valid and signed with the client's trusted CA. <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Examine which TLS version and cipher suites are offered. Compare the received values with the expected (pre-defined). - Repeat the test with different combinations of TLS version and cipher suites <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Examine the TLS certificate offered by MBF. Check if MBF does not choose a weaker cipher suite. <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Examine the TLS certificate offered by MBF for randomness per the requirements in FIPS-140-2 <p>Test 6 (hands-on):</p> <ul style="list-style-type: none"> - Examine the TLS certificate offered by MBF. Where a CA is operated in support of the TLS inspection within the MBF, it MUST clearly identify itself within the visible issuer properties (as defined in Section 4.1.2.4 of RFC 5280
<p>Test success criteria:</p>	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - The Application Flow decrypted by the MBF is not exposed outside the Service Provider's Security Functions in an unencrypted form or in an encrypted form that offers a lower level of confidentiality and integrity than the originally encrypted Application Flow. <p>Test 2 (hands-on):</p> <ul style="list-style-type: none"> - The TLS certificate offered by MBF is valid and signed with the client's trusted CA. <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - The MBF does not change the TLS protocol version for a TLS session as compared to the original client request. - TLS version and cipher suites are the same after re-encryption by MBF as originally provided by the simulated resource. - All replacement certificate properties, e.g., alternative server names, validity periods, and choices of cipher suites do not reduce the level of the security functionality of the properties of the certificate being replaced. <p>Test 4 (hands-on):</p>

	<ul style="list-style-type: none">- MBF does not choose a weaker cipher suite in the negotiation for a TLS session as compared to the TLS session without the MBF. <p>Test 5 (hands-on):</p> <ul style="list-style-type: none">- The TLS certificate offered by MBF is generated and regenerated with fresh, suitably random material per the requirements in FIPS-140-2. <p>Test 6 (hands-on):</p> <ul style="list-style-type: none">- Where a CA is operated in support of the TLS inspection within the MBF, it clearly identifies itself within the visible issuer properties (as defined in Section 4.1.2.4 of RFC 5280
--	--

Test case #18	Validate the targeted server certificate
Purpose:	Validate the targeted server certificate for the TLS session
Related requirement(s):	<p>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</p> <p>[R41] When performing TLS inspection within the MBF, it MUST be possible to use certificates that are backed by a CA where the trust path and issuer can be validated by users within the Subscriber's network who have installed the full certificate chain on their computer.</p> <p>[R42] The Service Provider MUST ensure that the certificate chain allowing for this validation to occur, as described in [R41], is made available to the Subscriber.</p> <p>[R46] The MBF MUST be capable of accepting a valid, signed Subscriber certificate for each TLS session between the MBF and the Subscriber's server.</p> <p>[R47] When an MBF is Enabled for a given Application Flow, the MBF MUST verify the validity of the targeted server certificate of the TLS session, as illustrated in Figure 3.</p> <p>[R48] When an invalid server certificate is detected, an MBF MUST be capable of Blocking the TLS session and notifying the client in the Subscriber's network of the invalid certificate.</p>
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. Two simulated web resources, accessible over TLS: <ul style="list-style-type: none"> - one with a legitimate trusted certificate (website 1) - one with a self-issued certificate (website 2)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule by adding the parameters of both web applications (website 1 and website 2) to the MBF Allow List <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - It should be confirmed that when performing TLS inspection within the MBF, it MUST be possible to use certificates that are backed by a CA where the trust path and issuer can be validated by users within the Subscriber's network who have installed the full certificate chain on their computer. <p>Test 2 (audit):</p> <ul style="list-style-type: none"> - It should be confirmed that the Service Provider provides an SD-WAN feature: the certificate chain allowing for this validation to occur, as described in [R41], is made available to the Subscriber.

	<p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the website 1 <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the website 2
<p>Test success criteria:</p>	<p>Test 1 (audit):</p> <p>When performing TLS inspection within the MBF, the certificates are backed by a CA, where the trust path and issuer can be validated by users within the Subscriber's network who have installed the full certificate chain on their computer.</p> <p>Test 2 (audit):</p> <p>When the Service Provider provides an SD-WAN feature: the certificate chain allowing for this validation to occur, as described in [R41], is made available to the Subscriber.</p> <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - The connection to Website 1 is successfully established - MBF is capable of accepting a valid, signed Subscriber certificate for each TLS session between the MBF and the Subscriber's server. <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - The connection to Website 2 is not established - When an invalid server certificate is detected, the MBF Blocks the TLS session, and notifies the client in the Subscriber's network of the invalid certificate. - SEN is triggered

Test case #19	Verify MBF IPPF filtering functionality
Purpose:	Verify the MBF IP, Port and Protocol Filtering (IPPF) requirements
Related requirement(s):	<p><i>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</i></p> <p><i>[R49] When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the IP, Port and Protocol Filtering Block List, the IP, Port and Protocol Filtering Allow List and the IP, Port and Protocol Filtering Quarantine List.</i></p> <p><i>[R50] When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R51] When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the IP, Port and Protocol Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R52] When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the IP, Port and Protocol Filtering Security Function MUST perform one of the following actions, based on agreement between the Service Provider and the Subscriber:</i></p> <ul style="list-style-type: none"> - Allow the subset of the Application Flow that matches a match criteria entry on the IP, Port and Protocol Filtering Allow List. - Allow the subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists, per the second bullet of [R51] - Block the subset of the Application Flow that matches a match criteria entry on the IP, Port and Protocol Filtering Block List. - Block the subset of the Application Flow that matches a match criteria entry on the IP, Port and Protocol Filtering Quarantine List. - Block the subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists, per the first bullet of [R51].
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated test web resource accessible over TLS (website 1) (URL 1, over HTTPS on port 443) - Simulated test web resource accessible over TLS (website 2) (URL 2, over HTTP on port 80) - Simulated test web resource accessible over TLS (website 3) (URL 3, over HTTP on port 4243)

	<ul style="list-style-type: none"> - Simulated test web resource accessible over TLS (website 4) (URL 4, over HTTPS on port 443)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule with the following rules: <ul style="list-style-type: none"> - Add web application 1 to the IPPF Filtering Allow List - Add web application 2 to the IPPF Filtering Block List - No explicit rule is created for the web application 3 - Add IPPF parameters of application 4 to the IPPF Filtering Quarantine list - Create a default action rule to block the subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists, per the first bullet of [R51]. <p>Test 1 (audit):</p> <p>Verify that when IP, Port and Protocol Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 2 (audit):</p> <p>Verify that when IP, Port and Protocol Filtering is Enabled for a given Application Flow, the IP, Port and Protocol Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 1) through the tested SD-WAN <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 2) through the tested SD-WAN <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 3) through the tested SD-WAN <p>Test 6 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 4) through the tested SD-WAN
Test success criteria:	<p>Test 1 (audit):</p> <p>When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the</p>

	<p>Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</p> <ul style="list-style-type: none">- Block the subset of the Application Flow- Allow the subset of the Application Flow <p>Test 2 (audit):</p> <p>When IP, Port and Protocol Filtering is Enabled for a given Application Flow, the IP, Port and Protocol Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the IP, Port and Protocol Filtering lists:</p> <ul style="list-style-type: none">- Block the subset of the Application Flow- Allow the subset of the Application Flow <p>Test 3 (hands-on):</p> <ul style="list-style-type: none">- Website 1 is accessed <p>Test 4 (hands-on):</p> <ul style="list-style-type: none">- Access to Website 2 is blocked- SEN is triggered <p>Test 5 (hands-on):</p> <ul style="list-style-type: none">- Access to Website 3 is blocked- SEN is triggered- New entry is created in the Quarantine list for website 3 <p>Test 6 (hands-on):</p> <ul style="list-style-type: none">- Access to Website 3 is blocked- SEN is triggered
--	--

Test case #20	Verify DNS filtering requirements
Purpose:	Verify the DNS Filtering requirements are satisfied
Related requirement(s):	<p><i>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</i></p> <p><i>[R53] When DNS Protocol Filtering is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the DNS Protocol Filtering Block List, the DNS Protocol Filtering Allow List and the DNS Protocol Filtering Quarantine List.</i></p> <p><i>[R54] When DNS Protocol Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R55] When DNS Protocol Filtering is Enabled for a given Application Flow, the DNS Protocol Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R56] When DNS Protocol Filtering is Enabled for a given Application Flow, the DNS Protocol Filtering Security Function MUST perform one of the following actions, based on agreement between the Service Provider and the Subscriber:</i></p> <ul style="list-style-type: none"> - Allow the subset of the Application Flow that matches a match criteria entry on the DNS Protocol Filtering Allow List. - Allow the subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists, per the second bullet of [R55]. - Block the subset of the Application Flow that matches a match criteria entry on the DNS Protocol Filtering Block List. - Block the subset of the Application Flow that matches a match criteria entry on the DNS Protocol Filtering Quarantine List. - Block the subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists, per the first bullet of [R55]. <p><i>[R57] The DNS Protocol Filtering Security Function MUST be capable of informing the DNS client in the Subscriber's network immediately of any DNS Message failure.</i></p> <p><i>[D4] When the DNS Protocol Filtering Security Function is Enabled for a given Application Flow, and when a DNS message in that Application Flow is Blocked, the DNS Protocol Filtering Security Function SHOULD send an appropriate DNS response code, per section 2.3 of RFC 6895, to the DNS client in the Subscriber's network.</i></p>
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated test web resource accessible over TLS (website 1) (over HTTPS on port 443)

	<ul style="list-style-type: none"> - Non-existing web resource (website 2) (over HTTPS on port 443) - Simulated DNS server 1 ("explicitly allowlisted") - Simulated DNS server 2 ("explicitly blocklisted") - Simulated DNS server 3 ("in quarantine") - Simulated DNS server 4 (unknown)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule with the following rules: <ul style="list-style-type: none"> - Add DNS server 1 to the DNS Filtering Allow List - Add DNS server 2 to the DNS Filtering Block List - Add DNS server 3 to the DNS Filtering Quarantine List - No explicit rule is created for DNS server 4 - Create a default action rule to block the subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists. <p>Test 1 (audit): Verify that when DNS Protocol Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 2 (audit): Verify that when DNS Protocol Filtering is Enabled for a given Application Flow, the DNS Protocol Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 1) through the tested SD-WAN while using DNS server 1 <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 1) through the tested SD-WAN while using DNS server 2 <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 1) through the tested SD-WAN while using DNS server 3 <p>Test 6 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (website 1) through the tested SD-WAN while using DNS server 4 <p>Test 7 (hands-on):</p>

	<ul style="list-style-type: none"> - Try to establish a connection to the non-existing web resource (website 2) through the tested SD-WAN while using DNS server 1
Test success criteria:	<p>Test 1 (audit): When DNS Protocol Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 2 (audit): When DNS Protocol Filtering is Enabled for a given Application Flow, the DNS Protocol Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the DNS Protocol Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (hands-on): - Website 1 may be accessed when the name resolution is done with DNS server 1 ("explicitly allowlisted")</p> <p>Test 4 (hands-on): - Access to Website 1 is blocked when the name resolution is done with DNS server 2 ("explicitly blocklisted") - SEN is triggered - Create a new entry in the Quarantine list matching DNS server 2 - DNS query is re-directed by the Service Provider to a web page that gives the reason(s) why the DNS query is Blocked</p> <p>Test 5 (hands-on): - Access to website 1 is blocked when the name resolution is done with DNS server 3 - SEN is triggered - DNS query is re-directed by the Service Provider to a web page that gives the reason(s) why the DNS query is Blocked</p> <p>Test 6 (hands-on): - Access to website 1 is blocked when the name resolution is done with DNS server 4 - SEN is triggered - Create new entry in the Quarantine list matching DNS server 4 - DNS query is re-directed by the Service Provider to a web page that gives the reason(s) why the DNS query is Blocked</p> <p>Test 7 (hands-on): - SEN is triggered, providing the details of the DNS failure message with the details of the unsuccessful DNS resolution</p>

Test case #21	Verify Domain Name Filtering requirements
Purpose:	Verify Domain Name Filtering requirements
Related requirement(s):	<p>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</p> <p>[R58] The Domain Name Filtering Security Function MUST be capable of using wildcard match criteria entries.</p> <p>[R59] The Service Provider MUST inform the Subscriber of the options regarding the use of wildcards for the Domain Name Filtering Security Function.</p> <p>[R60] When Domain Name Filtering is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the Domain Name Filtering Block List, the Domain Name Filtering Allow List and the Domain Name Filtering Quarantine List.</p> <p>[R61] When Domain Name Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>[R62] When Domain Name Filtering is Enabled for a given Application Flow, the Domain Name Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>[R63] When Domain Name Filtering is Enabled for a given Application Flow, the Domain Name Filtering Security Function MUST perform one of the following actions, based on agreement between the Service Provider and the Subscriber:</p> <ul style="list-style-type: none"> - Allow the subset of the Application Flow that matches a match criteria entry on the Domain Name Filtering Allow List. - Allow the subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists, per the second bullet of [R62]. - Block the subset of the Application Flow that matches a match criteria entry on the Domain Name Filtering Block List. - Block the subset of the Application Flow that matches a match criteria entry on the Domain Name Filtering Quarantine List. - Block the subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists, per the first bullet of [R62]. <p>[R64] The Domain Name Filtering Security Function MUST be capable of informing the client in the Subscriber's network immediately when access to a domain is Blocked.</p> <p>[D5] When access to a domain is Blocked, the client in the Subscriber's network SHOULD be immediately informed.</p>

Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated web application 1 ("explicitly allowlisted FQDN") (FQDN 1) - Simulated web application 2 ("explicitly allowlisted PQDN") (FQDN 2) - Simulated web application 3 ("explicitly blocklisted") (FQDN 3) - Simulated web application 4 ("in quarantine") (FQDN 4) - Simulated web application 5 (FQDN 5)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule with the following rules: <ul style="list-style-type: none"> - Add web application 1 to the Domain Filtering Allow List (when the application's domain name is "explicitly allowlisted FQDN") (FQDN 1) - Add web application 2 to the Domain Filtering Allow List (when the application's domain name is "explicitly allowlisted PQDN" with wildcard match criteria entry) (FQDN 2) - Add web application 3 to the Domain Filtering Block List (when the application's domain name is "explicitly blocklisted") (FQDN 3) - Add web application 4 to the Domain Filtering Quarantine List (FQDN 4) - No explicit rule is created for web application 5 (FQDN 5) - Create a default action rule when a subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists is to Block the subset of the Application Flow <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Verify if the Domain Name Filtering Security Function is capable of using wildcard match criteria entries. <p>Test 2 (audit):</p> <p>Verify that when Domain Name Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (audit):</p> <p>Verify that when Domain Name Filtering is Enabled for a given Application Flow, the Domain Name Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web resource (web application 1 with FQDN 1) through the tested SD-WAN <p>Test 5 (hands-on):</p>

	<p>- Try to establish a connection to the simulated web resource (web application 2 with FQDN 2) through the tested SD-WAN with a wildcard match criteria entry (PQDN)</p> <p>Test 6 (hands-on):</p> <p>- Try to establish a connection to the simulated web resource (web application 3 with FQDN 3) through the tested SD-WAN</p> <p>Test 7 (hands-on):</p> <p>- Try to establish a connection to the simulated web resource (web application 4 with FQDN 4) through the tested SD-WAN</p> <p>Test 8 (hands-on):</p> <p>- Try to establish a connection to the simulated web resource (web application 5 with FQDN 5) through the tested SD-WAN</p>
<p>Test success criteria:</p>	<p>Test1 (audit):</p> <p>The Domain Name Filtering Security Function uses wildcard match criteria entries.</p> <p>Test 2 (audit):</p> <p>When Domain Name Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (audit):</p> <p>When Domain Name Filtering is Enabled for a given Application Flow, the Domain Name Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Domain Name Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Website application 1 ("allowlisted FQDN") (FQDN 1) may be accessed <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Website application 2 ("allowlisted PQDN" with a wildcard match criteria entry) (PQDN) may be accessed <p>Test 6 (hands-on):</p> <p>Access to web application 3 ("blocklisted") (FQDN 3) is blocked</p> <ul style="list-style-type: none"> - SEN is triggered - New entry is created in the Quarantine list automatically matching the FQDN of web application 4 - In case of blocking the Domain Name, the query is re-directed by the Service Provider to a web page that gives the reason(s) why the original query is Blocked. <p>Test 7 (hands-on):</p> <ul style="list-style-type: none"> - Access to web application 4 is blocked

	<ul style="list-style-type: none">- SEN is triggered- In case of blocking the Domain Name, the query is re-directed by the Service Provider to a web page that gives the reason(s) why the original query is Blocked. <p>Test 8 (hands-on):</p> <ul style="list-style-type: none">- Access to web application is blocked- SEN is triggered- New entry is created in the Quarantine list automatically matching the FQDN of web application 5- In case of blocking the Domain Name, the query is re-directed by the Service Provider to a web page that gives the reason(s) why the original query is Blocked.
--	--

Test case #22	Verify URL Filtering requirements
Purpose:	Ensuring that the URL Filtering requirements
Related requirement(s):	<p>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</p> <p>[R65] The URL Filtering Security Function MUST be capable of using wildcard match criteria entries.</p> <p>[R66] The Service Provider MUST inform the Subscriber of the options regarding the use of wildcards for the URL Filtering Security Function.</p> <p>[R67] When URL Filtering is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the URL Filtering Block List, the URL Filtering Allow List and the URL Filtering Quarantine List.</p> <p>[R68] When URL Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>[R69] When URL Filtering is Enabled for a given Application Flow, the URL Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>[R70] When URL Filtering is Enabled for a given Application Flow, the URL Filtering Security Function MUST perform one of the following actions, based on agreement between the Service Provider and the Subscriber:</p> <ul style="list-style-type: none"> - Allow the subset of the Application Flow that matches a match criteria entry that is on the URL Filtering Allow List. - Allow the subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists, per the second bullet of [R69]. - Block the subset of the Application Flow that matches a match criteria entry on the URL Filtering Block List. - Block the subset of the Application Flow that matches a match criteria entry on the URL Filtering Quarantine List. - Block the subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists, per the first bullet of [R69]. <p>[R71] The URL Filtering Security Function MUST be capable of informing the client in the Subscriber's network immediately when access to a URL is Blocked.</p> <p>[D6] When URL Filtering is Enabled for a given Application Flow, and when access to a URL is Blocked, the client in the Subscriber's network SHOULD be immediately informed.</p>

Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated web application 1 ("allowlisted URL") (website 1) - Simulated web application 1 ("allowlisted URL") (website 2) - Simulated web application 2 ("blocklisted URL") (website 3) - Simulated web application 3 (website 4)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create a new security policy by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy rule with the following rules: <ul style="list-style-type: none"> - Add web application 1 to URL Filtering Allow List ("allowlisted URL") (website 1) - Add web application 2 to URL Filtering Allow List ("allowlisted URL" with wildcard match criteria entry) (website 2) - Add web application 3 to URL Filtering Block List ("blocklisted URL") (website 3) - No explicit rule is created for web application 3 (website 4) - Create a default action rule when a subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists is to Block the subset of the Application Flow <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Verify if the URL Filtering Security Function is capable of using wildcard match criteria entries. <p>Test 2 (audit):</p> <p>Verify that when URL Filtering is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 3 (audit):</p> <p>Verify that when URL Filtering is Enabled for a given Application Flow, the URL Filtering Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 1 (website 1) <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 1 (website 2) through the tested SD-WAN with a wildcard URL match criteria entry <p>Test 6 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 1 (website 3) <p>Test 7 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 1 (website 4)

Test success criteria:	<p>Test 1 (audit):</p> <ul style="list-style-type: none">- URL Filtering Security Function uses wildcard match criteria entries. <p>Test 2 (audit):</p> <p>When URL Filtering is Enabled for a given Application Flow, the Service Provider supports both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none">- Block the subset of the Application Flow- Allow the subset of the Application Flow <p>Test 3 (audit):</p> <p>When URL Filtering is Enabled for a given Application Flow, the URL Filtering Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the URL Filtering lists:</p> <ul style="list-style-type: none">- Block the subset of the Application Flow- Allow the subset of the Application Flow <p>Test 4 (hands-on):</p> <ul style="list-style-type: none">- Web application 1 (website 1) may be accessed <p>Test 5 (hands-on):</p> <ul style="list-style-type: none">- Web application 1 (website 2) may be accessed with a wildcard URL match criteria entry- SEN is triggered <p>Test 6 (hands-on):</p> <ul style="list-style-type: none">- Web application 1 (website 3) is blocked- SEN is triggered <p>Test 7 (hands-on):</p> <ul style="list-style-type: none">- Access to Web application 1 (website 4) is blocked- SEN is triggered
-------------------------------	--

Test case #23	Verify Malware Detection and Removal requirements
Purpose:	Verify Malware Detection and Removal requirements
Related requirement(s):	<p><i>[R16] A SEN MUST be issued whenever a subset of the Application Flow is Blocked or modified.</i></p> <p><i>[R72] When Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider MUST meet the mandatory requirements specified in Section 7.1 of this document relating to the Malware Detection and Removal Block List, the Malware Detection and Removal Allow List and the Malware Detection and Removal Quarantine List.</i></p> <p><i>[R73] When Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider MUST describe which kind of detection (e.g., signature scan, behavioral analysis or both) is performed.</i></p> <p><i>[R74] When Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider MUST support both of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal Filtering lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R75] When Malware Detection and Removal is Enabled for a given Application Flow, the Malware Detection and Removal Security Function MUST perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal lists:</i></p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow <p><i>[R76] When Malware Detection and Removal is Enabled for a given Application Flow, and when an Object in the Application 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:</i></p> <ul style="list-style-type: none"> - Block the Object and Block the associated subset of the Application Flow - Block the Object and Allow the associated subset of the Application Flow - Quarantine the Object and Block the associated subset of the Application Flow - Quarantine the Object and Allow the associated subset of the Application Flow - Remove Malware from the Object and Allow the associated subset of the Application Flow <p><i>[R77] The Service Provider MUST report which action is taken for detected Malware and make it available to the Subscriber via a SEN (see Section 7.2).</i></p>
Parameters:	<ul style="list-style-type: none"> - Access to the SD-WAN diagnostic/administrative functionality, available to Subscriber. - Simulated web application 1 (with a malicious signature 1 in the traffic) (website 1) - Simulated web application 2 (with a malicious signature 2 in the transmitted file) (website 2)

	- Simulated web application 3 (no malicious signatures) (website 3)
Testing approach:	Manual or automated
Testing process:	<p>Preparation:</p> <ul style="list-style-type: none"> - Create new security policies by using SD-WAN diagnostic/administrative functionality (manually or automatically) - Create and enable a new policy 1 with the following rule: If malicious traffic is detected (in the application traffic) the application flow is blocked. - Create and enable a new policy 2 with the following rule: If malicious traffic is detected (in a transmitted file) the application flow is not blocked but the malicious file is removed. <p>Test 1 (audit):</p> <ul style="list-style-type: none"> - Check when Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider MUST describe which kind of detection (e.g., signature scan, behavioral analysis or both) is performed. <p>Test 2 (audit):</p> <p>Verify that when Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider supports all of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow - Allow the subset of the Application Flow and remove the malicious content from the application's traffic <p>Test 3 (audit):</p> <p>Verify that when Malware Detection and Removal is Enabled for a given Application Flow, the Malware Detection and Removal Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow - Allow the subset of the Application Flow and remove the malicious content from the application's traffic <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 1 (website 1) - Send a valid traffic flow to an emulated web-site 1 in conjunction with Malware traffic. <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 2 (website 2) - Send a valid traffic flow to an emulated web-site 2 in conjunction with Malware traffic (transmission of a malicious file). <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - Try to establish a connection to the simulated web application 3 (website 3) - Send a valid traffic flow to an emulated web-site 3 with no Malware in the traffic.

<p>Test success criteria:</p>	<p>Test 1 (audit):</p> <ul style="list-style-type: none"> - When Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider describes which kind of detection (e.g., signature scan, behavioral analysis or both) is performed. <p>Test 2 (audit):</p> <p>When Malware Detection and Removal is Enabled for a given Application Flow, the Service Provider supports all of the following actions for a subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal Filtering lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow - Allow the subset of the Application Flow and remove the malicious content from the application's traffic <p>Test 3 (audit):</p> <p>When Malware Detection and Removal is Enabled for a given Application Flow, the Malware Detection and Removal Security Function is able to perform one of the following actions for each subset of the Application Flow that does not match a match criteria entry on any of the Malware Detection and Removal lists:</p> <ul style="list-style-type: none"> - Block the subset of the Application Flow - Allow the subset of the Application Flow - Allow the subset of the Application Flow and remove the malicious content from the application's traffic <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - It should not be possible to access web application 1 (website 1) - SEN should be triggered - Website 1 is moved to the Quarantine list - The application flow is blocked <p>Test 4 (hands-on):</p> <ul style="list-style-type: none"> - It should not be possible to access web application 2 (website 2) - SEN should be triggered - Website 2 is moved to the Quarantine list - The malicious content is removed from the data stream - The application flow is not blocked <p>Test 5 (hands-on):</p> <ul style="list-style-type: none"> - It should not be possible to access web application 3 (website 3) - SEN should NOT be triggered as there is no malware in the traffic
--------------------------------------	---

10 References

- [1] MEF 61.1, *IP Service Attributes*, January 2019
- [2] MEF 70.1, *SD-WAN Service Attributes and Services*, December 2020
- [3] MEF 88, *Application Security for SD-WAN Services*, November 2021

- [4] PCI-DSS: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
- [5] ITU-T X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, October 2016
- [6] IETF RFC 1035, DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION, November 1987
- [7] IETF RFC 1996, A Mechanism for Prompt Notification of Zone Changes (DNS NOTIFY), August 1996
- [8] IETF RFC 2119, *Key words for use in RFCs to Indicate Requirement Levels*, March 1997
- [9] IETF RFC 2818, *HTTP Over TLS*, May 2000
- [10] IETF RFC 3339, *Date and Time on the Internet: Timestamps*, July 2002
- [11] IETF RFC 3507, *Internet Content Adaptation Protocol (ICAP)*, April 2003
- [12] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*, January 2005
- [13] IETF RFC 4122, *A Universally Unique Identifier (UUID) URN Namespace*, July 2005
- [14] IETF RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*, September 2005
- [15] IETF RFC 4648, *The Base16, Base32, and Base64 Data Encodings*, October 2006
- [16] IETF RFC 4703, *Resolution of Fully Qualified Domain Name (FQDN) Conflicts among Dynamic Host Configuration Protocol (DHCP) Clients*, October 2006
- [17] IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*, August 2008
- [18] IETF 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008
- [19] IETF RFC 6797, *HTTP Strict Transport Security (HSTS)*, November 2012
- [20] IETF RFC 6895, *Domain Name System (DNS) IANA Considerations*, April 2013
- [21] IETF RFC 6960, *X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP*, June 2013
- [22] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*, June 2014
- [23] IETF RFC 7540, *Hypertext Transfer Protocol Version 2 (HTTP/2)*, May 2015

- [24] IETF RFC 7686, *The ".onion" Special-Use Domain Name*, October 2015
- [25] IETF RFC 7858, *Specification for DNS over Transport Layer Security (TLS)*, May 2016
- [26] IETF RFC 7970, *The Incident Object Description Exchange Format Version 2*, November 2016
- [27] IETF RFC 8174, *Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words*, May 2017
- [28] IETF RFC 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*, August 2018
- [29] IETF RFC 8484, *DNS Queries over HTTPS (DoH)*, October 2018
- [30] <https://datatracker.ietf.org/wg/quic/documents/>
- [31] ETSI TS 103 523-3 V1.2.1, *Technical Specification, CYBER; Middlebox Security Protocol; Part 3: Enterprise Transport Security*, March 2019
- [32] NIST Special Publication 800-53 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations, Information System Monitoring*. [NIST 800-53/Rev4/control/SI-4](#)
- [33] NIST Special Publication 800-94, *Guide to Intrusion Detection and prevention Systems (IDPS)*, February 2007

Appendix A SD-WAN Performance Certification Test Cases Description

(IETF Benchmarking Methodology for Network Security Device Performance (draft-ietf-bmwg-ngfw-performance-09))

A.1 Introduction

This Appendix includes a set of optional test cases that enable a managed service provider or security function vendor to assess the security performance for one or more security functions specified in MEF 88. Since MEF 88 does not explicitly specify security performance requirements, these test cases are not included in the MEF Secure SD-WAN Certification Test Suite but are provided to enable service providers to assess the performance impact of the security functions that they deploy.

The security performance testing methodology has been adopted from the IETF Benchmarking Methodology for Network Security Device Performance: **draft-ietf-bmwg-ngfw-performance-09**

<https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/>

The test cases specified in this IETF Internet Draft have been adopted and implemented by the NetSecOPEN organization: www.netsecopen.org

The NetSecOPEN forum has defined a set of standardized test methodologies to validate different aspects of modern security devices and security controls. This encompasses key performance and availability tests as well as specific security efficacy testing using specified attack constructs. As a draft IETF standard, test definitions and parameters are subject to change until formal ratification.

For the purposes of the MEF131 SD-WAN only specific NetSecOPEN **performance tests** will be defined.

NetSecOPEN performance test cases are summarized below:

- **Test case #C-1: Verify Application Layer Performance of TCP/HTTP Connections Per Second**
Using HTTP traffic, determine the sustainable TCP connection establishment rate supported by the DUT/SUT under different throughput load conditions.
- **Test case #C-2: Verify Application Layer Performance of HTTP Throughput**
Determine the sustainable inspected throughput of the DUT/SUT for HTTP transactions varying the HTTP response object size.
- **Test case #C-3: Verify Application Layer Performance of Concurrent TCP/HTTP Connection Capacity**
Validate the maximum number of serviceable TCP/HTTP connection capacity. The purpose of this test is to determine the serviceable TCP/HTTP connections specified Security Function.

- **Test case #C-4: Verify Application Layer Performance of TCP/HTTPS Connections Per Second**
Using HTTPS traffic, determine the sustainable TCP connection establishment rate supported by the DUT/SUT under different throughput load conditions.
- **Test case #C-5: Verify Application Layer Performance of HTTPS Throughput**
Determine the sustainable inspected throughput of the DUT/SUT for HTTPS transactions varying the HTTP response object size
- **Test case #C-6: Verify Application Layer Performance of Concurrent TCP/HTTPS Connection Capacity**
Validate the maximum number of serviceable TCP/HTTPS connection capacity. The purpose of this test is to determine the serviceable TCP/HTTPS connections specified Security Function.

The security performance test cases are defined in the tables below.

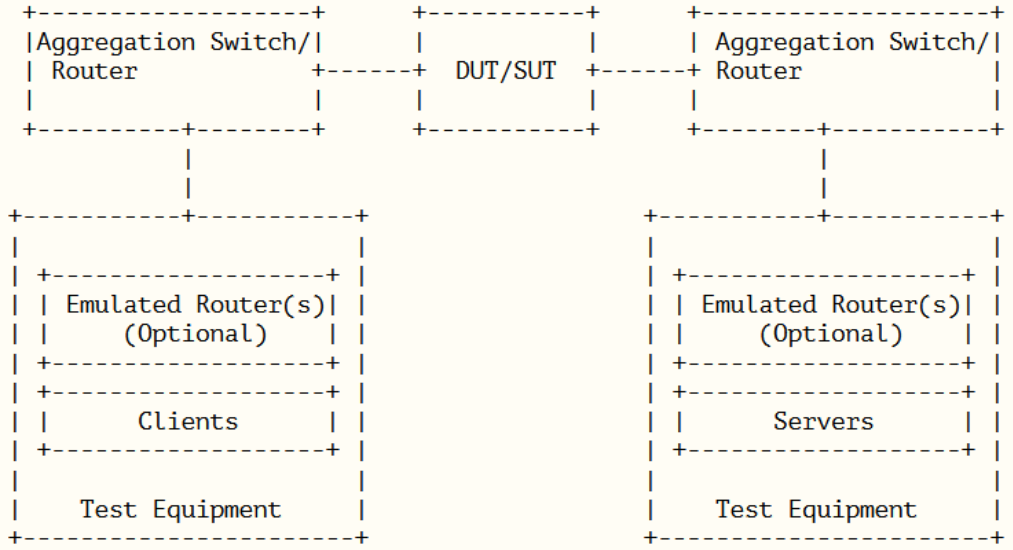
Table C-1 summarizes the requirements specified in the IETF Benchmarking Methodology for Network Security Device Performance (v9).

Table conventions are provided in TBD.

Table 4 – IETF Benchmarking Methodology for Network Security Device Performance Requirements Coverage

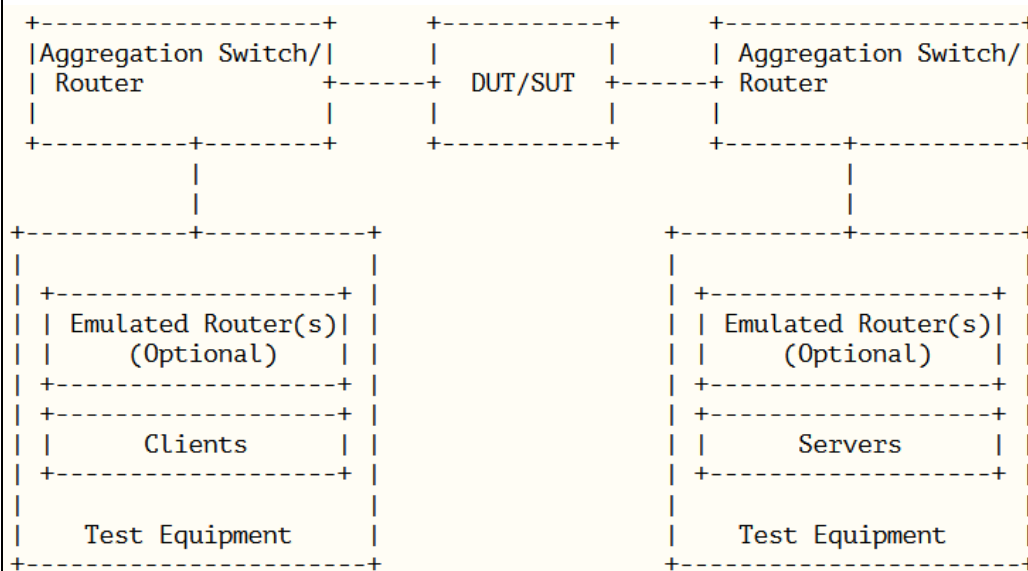
Test Case	IETF Benchmarking Methodology for Network	Notes
#C-1	Section 7.2	
#C-2	Section 7.3	
#C-3	Section 7.5	
#C-4	Section 7.6	
#C-5	Section 7.7	
#C-6	Section 7.9	

Test case #C-1	Verify Application Layer Performance of TCP/HTTP Connections Per Second
Purpose:	<p>TCP/HTTP Connections Per Second</p> <p>The purpose of this test is to assess the TCP/HTTP 1.1 Connection Establishment rate for the specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p> <p>In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.</p>
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.2</p> <p>https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <p><i>Separate tests must be run with different object sizes to validate connection rate performance with</i></p> <ul style="list-style-type: none"> ○ 1 KByte ○ 16 KByte ○ 64 KByte <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security policies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client-side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server-side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • IP addressing should be IPv4 • Tests will be done using HTTP 1.1 on Port 80 • HTTP traffic flow behavior will be based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.3

	<ul style="list-style-type: none"> Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3
Basic diagram:	 <p>draft-ietf-bmwg-ngfw-performance-09 Section 4.1</p>
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 7.2</p> <ul style="list-style-type: none"> Initial test maximum value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario

	<ul style="list-style-type: none"> • Separate tests and results will be run for each object return size. 1 KByte, 16 KByte, 64 KByte • HTTP 1.1 Payload can be random or pseudo random data • Each connection should close with FIN after each HTTP transaction completes • Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.2.3.3 • Each test will be run with the target objective TCP/HTTP connections per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.2.4.2
Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum TCP/HTTP Connections and Transactions per second for each object return size.</p> <p>TCP Connections Per Second</p> <ul style="list-style-type: none"> • The average number of successfully established TCP connections per second between hosts across the DUT/SUT, or between hosts and the DUT/SUT. The TCP connection must be initiated via a TCP three-way handshake (SYN, SYN/ACK, ACK). Then the HTTP session data is sent. <p>Application Transactions Per Second</p> <ul style="list-style-type: none"> • The average number of successfully completed HTTP transactions per second. For a particular transaction to be considered successful, all data must have been transferred in its entirety. <p>Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.2.3.3</p>

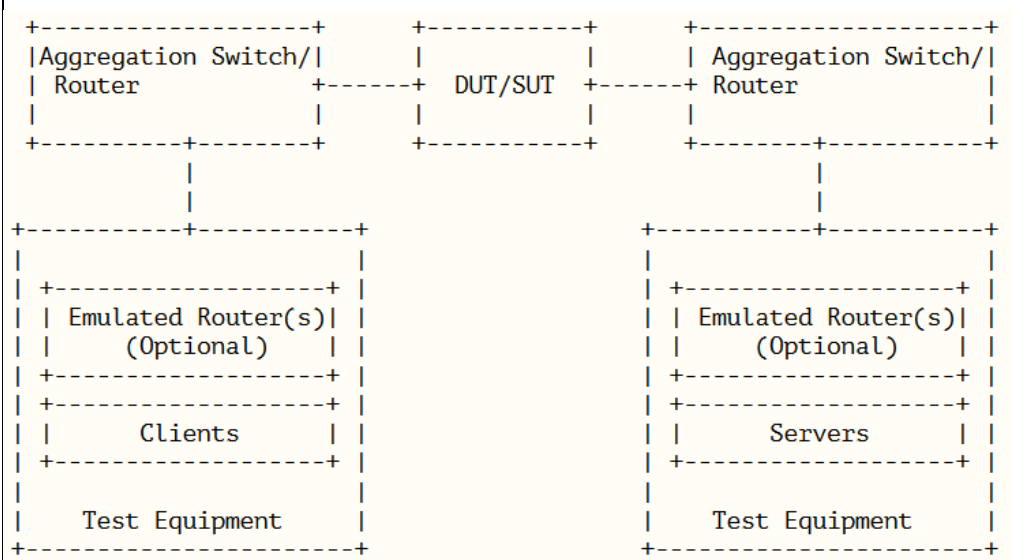
Test case #C-2	Verify Application Layer Performance of HTTP Throughput
Purpose:	<p>Validate maximum HTTP throughput</p> <p>The purpose of this test is to assess the maximum HTTP throughput rate for the specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p> <p>In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.</p>
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.3</p> <p>https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <p><i>Separate tests must be run with different object sizes to validate connection rate performance with</i></p> <ul style="list-style-type: none"> ○ 1 KByte ○ 16 KByte ○ 64 KByte ○ 256 KByte <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security policies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • IP addressing should be IPv4 • Tests will be done using HTTP 1.1 on Port 80 • HTTP traffic flow behavior will be based draft-ietf-bmwg-ngfw-performance-09 section 4.3.3

	<ul style="list-style-type: none"> Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3
Basic diagram:	 <p>draft-ietf-bmwg-ngfw-performance-09 Section 4.1</p>
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 7.3</p> <ul style="list-style-type: none"> Initial test maximum value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario

	<ul style="list-style-type: none"> Separate tests and results will be run for each object return size. 1 KByte, 16 KByte, 64 KByte, and 256 KByte HTTP 1.1 Payload can be random or pseudo random data Each connection should close with FIN after each HTTP transaction completes Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.3.3.3 Each test will be run with the target objective HTTP throughput per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.3.4.2
Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum TCP/HTTP Connections and Transactions per second for each object return size.</p> <p>HTTP Inspected Throughput</p> <ul style="list-style-type: none"> The number of bits per second of examined and allowed traffic a network security device is able to transmit to the correct destination interface(s) in response to a specified offered load. The throughput benchmarking tests defined in Section 7 SHOULD measure the average Layer 2 throughput value when the DUT/SUT is "inspecting" traffic. This document recommends presenting the inspected throughput value in Gbit/s rounded to two places of precision with a more specific Kbit/s in parenthesis. Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.3.3.3

Test case #C-3	Verify Application Layer Performance of Concurrent TCP/HTTP Connection Capacity
Purpose:	<p>Validate the maximum number of serviceable TCP/HTTP connection capacity</p> <p>The purpose of this test is to determine the serviceable TCP/HTTP connections specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p>

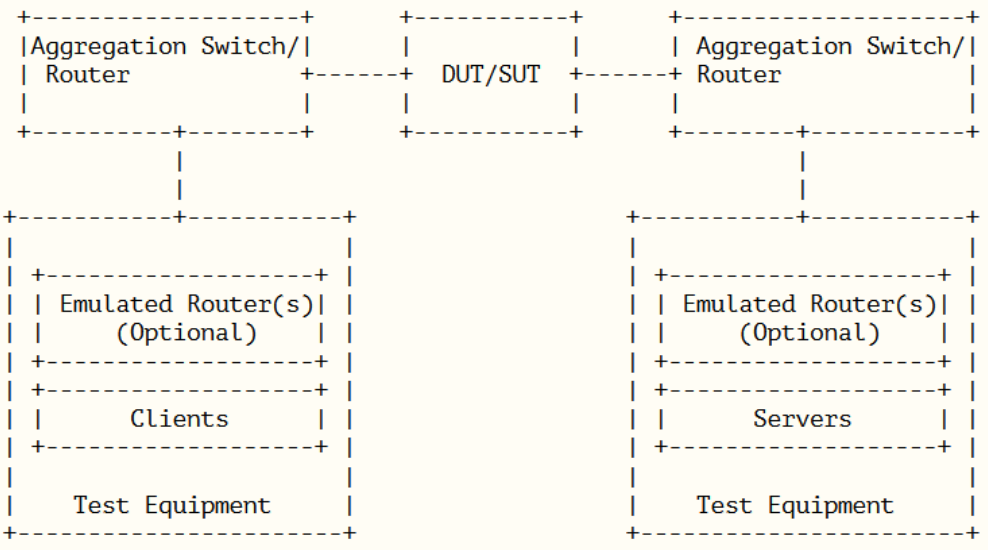
	In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.5</p> <p>https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security policies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • IP addressing should be IPv4 • Tests will be done using HTTP 1.1 on Port 80 • HTTP traffic flow behavior will be based draft-ietf-bmwg-ngfw-performance-09 section 4.3.3 • Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 • Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 • Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3

Basic diagram:	 <p>draft-ietf-bmwg-ngfw-performance-09 Section 4.1</p>
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 7.5</p> <ul style="list-style-type: none"> Initial test maximum connectivity value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario Test parameters are based draft-ietf-bmwg-ngfw-performance-09 Section 7.5.3.2 HTTP 1.1 Payload can be random or pseudo random data Each connection should close with FIN after each HTTP transaction completes Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.5.3.3 Each test will be run with the target objective HTTP throughput per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.5.4.2

Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum serviceable TCP/HTTP connection capacity.</p> <ul style="list-style-type: none">• Configure test equipment to establish "Initial concurrent TCP connections" defined in draft-ietf-bmwg-ngfw-performance-09 section 7.5.3.2. Except ramp up time, the traffic load profile SHOULD be defined as described in draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 During the sustain phase, the DUT/SUT SHOULD reach the "Initial concurrent TCP connections".• The measured KPIs during the sustain phase MUST meet all the test results validation criteria defined in draft-ietf-bmwg-ngfw-performance-09 section 7.5.3.3.

Test case #C-4	Verify Application Layer Performance of TCP/HTTPS Connections Per Second
Purpose:	<p>TCP/HTTPS Encrypted Connections Per Second</p> <p>The purpose of this test is to assess the TCP/HTTPS 1.1 Connection Establishment rate for the specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p> <p>In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.</p>
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.6</p> <p>https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <p><i>Separate tests will be run with different object sizes to validate connection rate performance with</i></p> <ul style="list-style-type: none"> ○ 1 KByte ○ 16 KByte ○ 64 KByte <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security poliicies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • From draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3 for encrypted traffic, the following attributes SHALL define the negotiated encryption parameters. TLS record size MAY be optimized for the HTTPS response object size up to a record size of 16 KByte. Each client connection MUST perform a full handshake with server certificate and MUST NOT use session reuse or resumption.

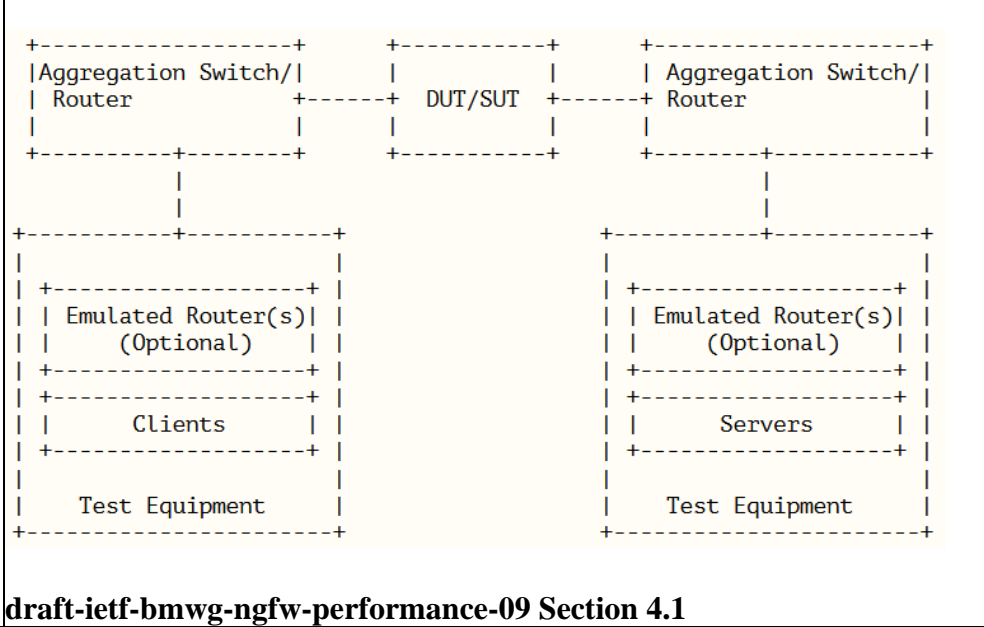
	<ul style="list-style-type: none"> For the purposes of this performance test a TLS 1.2 cipher will be used. The following TLS 1.2 supported ciphers and keys are RECOMMENDED to use for HTTPS based benchmarking tests defined in draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3. ECHDE-ECDSA-AES128-GCM-SHA256 with Prime256v1 (Signature Hash) Algorithm: ecdsa_secp256r1_sha256 and Supported group: secp256r1) ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 (Signature Hash) Algorithm: rsa_pkcs1_sha256 and Supported group: secp256) ECDHE-ECDSA-AES256-GCM-SHA384 with Secp521 (Signature Hash) Algorithm: ecdsa_secp384r1_sha384 and Supported group: secp521r1) ECDHE-RSA-AES256-GCM-SHA384 with RSA 4096 (Signature Hash) Algorithm: rsa_pkcs1_sha384 and Supported group: secp256) IP addressing should be IPv4 Tests will be done using HTTPS 1.1 on Port 443 HTTPS traffic flow behavior will be based draft-ietf-bmwg-ngfw-performance-09 section 4.3.3 Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3

Basic diagram:	 <p>The diagram illustrates a network topology for testing. A central DUT/SUT (Device Under Test/Subject Under Test) is connected to two Aggregation Switch/Routers. Each Aggregation Switch/Router is connected to a set of Emulated Router(s) (Optional), Clients, Servers, and Test Equipment. The connections are shown with dashed lines and plus signs at the endpoints.</p> <p>draft-ietf-bmwg-ngfw-performance-09 Section 4.1</p>
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 section 7.6</p> <ul style="list-style-type: none"> Target connections per second: Initial test maximum value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario Separate tests and results will be run for each object return size. 1 KByte, 16 KByte, 64 KByte HTTPS 1.1 Payload can be random or pseudo random data A single and consistent cipher for all object return sizes will be selected from TLS 1.2 section draft-ietf-bmwg-ngfw-performance-09 Section 4.3.1.3 will be used and properly documented with test results Each connection should close with FIN after each transaction Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.6.3.3

	<ul style="list-style-type: none"> Each test will be run with the target objective TCP/HTTPS connections per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.6.4.2
Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum TCP/HTTPS Connections and Transactions per second for each object return size.</p> <p>TCP Connections Per Second</p> <ul style="list-style-type: none"> The average number of successfully established TCP connections per second between hosts across the DUT/SUT, or between hosts and the DUT/SUT. The TCP connection must be initiated via a TCP three-way handshake (SYN, SYN/ACK, ACK). Then the HTTPS session data is sent. <p>Application Transactions Per Second</p> <ul style="list-style-type: none"> The average number of successfully completed HTTPS transactions per second. For a particular transaction to be considered successful, all data must have been transferred in its entirety. <p>TLS Handshake Rate</p> <ul style="list-style-type: none"> The average number of successfully established TLS connections per second between hosts across the DUT/SUT, or between hosts and the test environment. <p>Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.6.3.3</p>

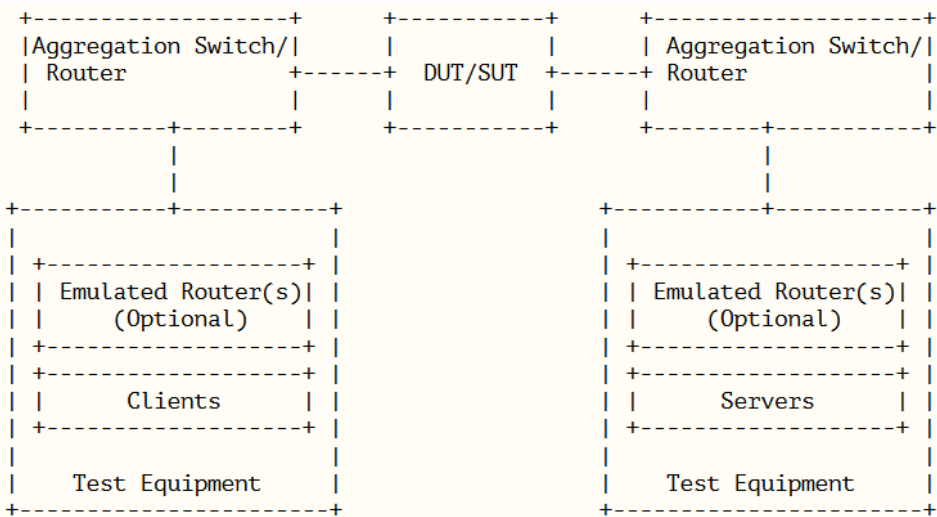
Test case #C-5	Verify Application Layer Performance of HTTPS Throughput
Purpose:	<p>Validate maximum HTTPS throughput</p> <p>The purpose of this test is to assess the maximum HTTPS throughput rate for the specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p> <p>In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.</p>
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.7</p> <p>https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <p><i>Separate tests must be run with different object sizes to validate connection rate performance with</i></p> <ul style="list-style-type: none"> ○ 1 KByte ○ 16 KByte ○ 64 KByte ○ 256 KByte <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security policies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • From draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3 for encrypted traffic, the following attributes SHALL define the negotiated encryption parameters. TLS record size MAY be optimized for the HTTPS response object size up to a record size of 16 KByte. Each client connection MUST perform a full handshake

	<p>with server certificate and MUST NOT use session reuse or resumption.</p> <ul style="list-style-type: none"> For the purposes of this performance test a TLS 1.2 cipher will be used. The following TLS 1.2 supported ciphers and keys are RECOMMENDED to use for HTTPS based benchmarking tests defined in draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3. <ul style="list-style-type: none"> ECHDE-ECDSA-AES128-GCM-SHA256 with Prime256v1 (Signature Hash) Algorithm: ecdsa_secp256r1_sha256 and Supported group: secp256r1) ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 (Signature Hash) Algorithm: rsa_pkcs1_sha256 and Supported group: secp256) ECDHE-ECDSA-AES256-GCM-SHA384 with Secp521 (Signature Hash) Algorithm: ecdsa_secp384r1_sha384 and Supported group: secp521r1) ECDHE-RSA-AES256-GCM-SHA384 with RSA 4096 (Signature Hash) Algorithm: rsa_pkcs1_sha384 and Supported group: secp256) Tests will be done using HTTPS 1.1 on Port 443 IP addressing should be IPv4 HTTPS traffic flow behavior will be based draft-ietf-bmwg-ngfw-performance-09 section 4.3.3 Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3

Basic diagram:	 <p>The diagram illustrates a network topology for testing. A central DUT/SUT (Device Under Test/Subject Under Test) is connected to two Aggregation Switch/Routers. Each switch is connected to a set of Emulated Router(s) (Optional), Clients, Servers, and Test Equipment. The diagram is divided into two symmetrical halves, each representing a different side of the network.</p> <p>draft-ietf-bmwg-ngfw-performance-09 Section 4.1</p>
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 7.7</p> <ul style="list-style-type: none"> Initial test maximum value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario Separate tests and results will be run for each object return size. 1 KByte, 16 KByte, 64 KByte, and 256 KByte HTTP 1.1 Payload can be random or pseudo random data Each connection should close with FIN after each HTTP transaction completes Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.7.3.3 Each test will be run with the target objective HTTP throughput per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.7.4.2

Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum HTTPS for each object return size.</p> <p>HTTPS Inspected Throughput</p> <ul style="list-style-type: none">• The number of bits per second of examined and allowed traffic a network security device is able to transmit to the correct destination interface(s) in response to a specified offered load. The throughput benchmarking tests defined in on draft-ietf-bmwg-ngfw-performance-09 Section 7 SHOULD measure the average Layer 2 throughput value when the DUT/SUT is "inspecting" traffic. This document recommends presenting the inspected throughput value in Gbit/s rounded to two places of precision with a more specific Kbit/s in parenthesis.• Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.7.3.3

Test case #C-6	Verify Application Layer Performance of Concurrent TCP/HTTPS Connection Capacity
Purpose:	<p>Validate the maximum number of serviceable TCP/HTTPS connection capacity</p> <p>The purpose of this test is to determine the serviceable TCP/HTTPS connections specified Security Function (specified in MEF 88 Sec 9 'Security Function').</p> <p>In the Secure SD-WAN Certification Test Requirements document, it is important to relate the environment performance test to the MEF SD-WAN concepts.</p>
Related requirement(s):	<p>This test is based on draft-ietf-bmwg-ngfw-performance-09 7.9 https://datatracker.ietf.org/doc/draft-ietf-bmwg-ngfw-performance/</p> <ul style="list-style-type: none"> • If test traffic will be inspected by NGFW or IPD/IDP security policies the test environment configuration parameters should follow draft-ietf-bmwg-ngfw-performance-09 4.2 • Client side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.1 and 4.3.1.2 • Server side TCP stack and IP addressing should be set to draft-ietf-bmwg-ngfw-performance-09 section 4.3.2.1 and 4.3.2.2 • IP addressing should be IPv4 • Tests will be done using HTTP 1.1 on Port 443 • From draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3 for encrypted traffic, the following attributes SHALL define the negotiated encryption parameters. TLS record size MAY be optimized for the HTTPS response object size up to a record size of 16 KByte. Each client connection MUST perform a full handshake with server certificate and MUST NOT use session reuse or resumption. • For the purposes of this performance test a TLS 1.2 cipher will be used. The following TLS 1.2 supported ciphers and keys are RECOMMENDED to use for HTTPS based benchmarking tests defined in draft-ietf-bmwg-ngfw-performance-09 section 4.3.1.3.

	<ul style="list-style-type: none"> ○ ECHDE-ECDSA-AES128-GCM-SHA256 with Prime256v1 (Signature Hash) Algorithm: ecdsa_secp256r1_sha256 and Supported group: secp256r1) ○ ECDHE-RSA-AES128-GCM-SHA256 with RSA 2048 (Signature Hash) Algorithm: rsa_pkcs1_sha256 and Supported group: secp256) ○ ECDHE-ECDSA-AES256-GCM-SHA384 with Secp521 (Signature Hash) Algorithm: ecdsa_secp384r1_sha384 and Supported group: secp521r1) ○ ECDHE-RSA-AES256-GCM-SHA384 with RSA 4096 (Signature Hash) Algorithm: rsa_pkcs1_sha384 and Supported group: secp256) • HTTP traffic flow behavior will be based draft-ietf-bmwg-ngfw-performance-09 section 4.3.3 • Traffic load ramp up, sustain, and ramp down phases are based on draft-ietf-bmwg-ngfw-performance-09 section 4.3.4 • Reporting should indicate all attitudes of DUT/SUT as outlined draft-ietf-bmwg-ngfw-performance-09 section 6.1 • Report details and KPI should include attributes in draft-ietf-bmwg-ngfw-performance-09 sections 6.2 and 6.3
Basic diagram:	 <pre> +-----+ +-----+ +-----+ Aggregation Switch/ DUT/SUT Aggregation Switch/ Router +-----+ Router +-----+ +-----+ +-----+ +-----+ +-----+ +-----+ +-----+ Emulated Router(s) Emulated Router(s) (Optional) (Optional) +-----+ +-----+ Clients Servers +-----+ +-----+ Test Equipment Test Equipment +-----+ +-----+ +-----+ +-----+ +-----+ </pre>

	draft-ietf-bmwg-ngfw-performance-09 Section 4.1
Testing approach:	Manual or Automated
Testing process:	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 7.9</p> <ul style="list-style-type: none"> Initial test maximum connectivity value should be defined from product vendor specifications, or the value defined based on requirement for a specific deployment scenario Test parameters are based draft-ietf-bmwg-ngfw-performance-09 section 7.9.3.2 HTTP 1.1 Payload can be random or pseudo random data Each connection should close with FIN after each HTTP transaction completes Test results validation criteria will be based on draft-ietf-bmwg-ngfw-performance-09 Section 7.9.3.3 Each test will be run with the target objective HTTP throughput per section as described in draft-ietf-bmwg-ngfw-performance-09 Section 7.9.4.2
Testing Result(s)	<p>As outlined in draft-ietf-bmwg-ngfw-performance-09 Section 6.3, the objective of this test is to assess maximum serviceable TCP/HTTP connection capacity.</p> <ul style="list-style-type: none"> Configure test equipment to establish "Initial concurrent TCP connections" defined in draft-ietf-bmwg-ngfw-performance-09 section 7.9.3.2. Except ramp up time, the traffic load profile SHOULD be defined as described in draft-ietf-bmwg-ngfw-performance-09 section 4.3.4. During the sustain phase, the DUT/SUT SHOULD reach the "Initial concurrent TCP connections". The measured KPIs during the sustain phase MUST meet all the test results validation criteria defined in draft-ietf-bmwg-ngfw-performance-09 section 7.9.3.3.

