Mplify Standard

Mplify 169

Security Service Edge Framework

February 2026

Disclaimer

The information in this publication is freely available for reproduction and use by any recipient and is believed to be accurate as of its publication date. Such information is subject to change without notice and Mplify Alliance (Mplify) is not responsible for any errors. Mplify does not assume responsibility to update or correct any information in this publication. No representation or warranty, expressed or implied, is made by Mplify concerning the completeness, accuracy, or applicability of any information contained herein and no liability of any kind shall be assumed by Mplify 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. Mplify 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 Mplify member which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor

b) any warranty or representation that any Mplify 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 Mplify member and the recipient or user of this document.

Implementation or use of specific Mplify standards, specifications, or recommendations will be voluntary, and no Member shall be obliged to implement them by virtue of participation in Mplify Alliance. Mplify is a global alliance of network, cloud, cybersecurity, and enterprise organizations working together to accelerate the AI-powered digital economy through standardization, automation, certification, and collaboration. Mplify does not, expressly or otherwise, endorse or promote any specific products or services.

Table of Contents

List of Figures

List of Tables

1 List of Contributing Members

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

- Bell Canada
- Cisco
- Equinix
- Palo Alto Networks

2 Abstract

This document defines Service Attributes and a framework that can be used as the basis for a Security Service Edge (SSE) offering. It is not intended as a stand-alone, implementable entity, describing SSE services or SSE products. This document draws mainly on the Security Functions defined in MEF 138 [7] and identifies how these Security Functions serve as building blocks for Security Solutions that are used to provide an SSE offering.

The Framework includes, but is not limited to, Secure Access, Full Proxy, Forward Proxy, Reverse Proxy, Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Secure Gateway (SG), and other Security Solutions and Security Functions that enable SSE as well as an extended set of capabilities and a variety of example use-cases.

3 Terminology and Abbreviations

This section defines the terms used in this document. In many cases, the normative definitions to terms are found in other documents. In these cases, the third column is used to provide the reference that is controlling, in other Mplify or external documents.

In addition, terms defined in MEF 138 [7] and MEF 118.1 [6] are included in this document by reference and are not repeated in the table below. It is expected that the reader has familiarity with these documents.

Term	Definition	Reference
Access Control	A security technique that regulates who or what can view or use resources in a computing environment.	This document
CASB Action	The function that is performed such as Store, Upload, and Download	This document
Data Integrity	The Security Function that examines Sessions to certain supported applications and determines if the CASB Actions included in those Sessions are allowed or blocked.	Adapted from Mplify 117.1 [5]
Data Privacy	A process by which the Subscriber's data is protected by Security Functions and Security Solutions such that it is transmitted to only appropriate Actors, contains only the appropriate information allowed to be shared with given Actor, and that all of this is controlled by SSE Policy	This document
Data Protection	The process by which the Subscriber Data is protected from malicious threat injection, compromise, or infiltration and is controlled by SSE Policy.	This document
Data Security	A process by which the Subscriber's data is protected by Security Functions and Security Solutions such that it cannot be intercepted and disclosed by unauthorized Actors, that it is transmitted to only appropriate Actors, and that all of this is controlled by SSE Policy.	This document
Firewall as a Service	A firewall solution delivered as a cloud-based service	This document
Forward Proxy	A Proxy where the Subject Actor's session is terminated and a new session initiated to mask the Subject Actor from the Target Actor. Additionally, Security Policies can be applied at the Proxy level to protect the Subject Actor from malicious traffic returned by the Target Actor and limit what the Subject Actor can send to the Target Actor.	This document
Full Proxy	A Proxy that supports both Forward and Reverse Proxies.	This document

Term	Definition	Reference
Identity Management	A function that is used by an SSE Service that adopts this SSE Framework to identify and Authenticate the Subject Actor (and possibly the Target Actor) for which Policies are applied.	Adapted from MEF 118.1 [6]
Proxy	A Security Function that terminates/originates a flow from a Subject Actor and terminates/originates a flow from a Target Actor.	This document
Reverse Proxy	A Proxy where the Subject Actor's session is terminated and a new session initiated to the Target Actor. Additionally, Security Policies can be applied at the Proxy level to protect the Target Actor from malicious traffic sent by the Subject Actor and limit what data and transactions can be exchanged between the Target Actor and the Subject Actor.	This document
Safeguarding Data	A method of using Security Functions to protect data	This document
Secure Access	The ability to restrict Subject Actors from accessing Target Actors using one or more Policies or rules. It is applicable to both Private and Public access	This document
Secure Gateway	A Security Solution that provides a method that prevents access to data without the correct permissions contained within applicable SSE Policies.	This document
Secure Tunnel	A secure network connection either between the Subject Actor and the SSE or the SSE and the Subscriber Network/Target Actor over which certain IP routes are advertised for access via Secure Private Access.	This document
Security Service Edge	A collection of Security Functions and Security Solutions that is aimed to secure any Subject Actor access of any Target Actor anywhere.	This document
Security Solution	An implementation of one or more Security Functions intended to address a specific security threat	This document
SSE Policy	The instructions for SSE operation	This document
SSE Policy End Point	The point where an SSE Policy is identified, applied, or enforced.	This document
SSE Framework	The set of Security Functions and Security Solutions that define an SSE	This document
SSE Interface Termination	A termination point such as an SSE UNI or SSE NNI	This document
SSE NNI	Used to interconnect the SSE to other SASE functionalities , (e.g. Zero Trust, or SD-WAN)	This document
SSE Subscriber	A Subscriber who is using an SSE	This document

Term	Definition	Reference
SSE UNI	The demarcation of responsibility between the Subscriber and SSE Service Provider	This document
Subscriber Network	A set of connections, functions and solutions that make up the Subscribers data service.	This document

Table 1 – Terminology

Abbreviation	Definition	Reference
CASB	Cloud Access Security Broker	This document
DLP	Data Loss Prevention	This document
SG	Secure Gateway	This document
SSE	Security Service Edge	This document

Table 2 – Abbreviations

4 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 [2], RFC 8174 [3]) 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**.**

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

5 Numerical Prefix Conventions

This document uses the prefix notation to indicate multiplier values as shown in Table 3.

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

Table 3 – Numerical Prefix Conventions

6 Introduction

Security Service Edge (SSE) has been described as a collection of Security Functions and Security Solutions. This document is intended to remove any ambiguity regarding what is included in an SSE Framework. A Security Solution implements one or more Security Functions intended to solve a specific security threat. Many of the Security Functions are taken directly from MEF 138 [7]. This document defines the specific Security Functions and Security Solutions that make up an SSE Framework. The SSE framework does not specify a single implementation. Multiple Security Functions and Security Solutions from different vendors can be inter-worked to provide the SSE framework items and solutions specified in this document.

This document is structured as follows:

- Security Functions that make up Security Solutions (section 7)
- SSE use cases and associated Security Functions (section 8)
- SSE Framework (section 9)

A set of use cases addressed by an SSE Framework are discussed. These include ways that an SSE Framework can provide:

- Secure Access – Access controlled via a Policy
  - Private access
  - Public access
- Safeguarding Data - Cloud Access Security Broker (CASB), Data Loss Prevention (DLP), Secure Gateway (SG), and other security functions
  - Data Security – protecting digital information from unauthorized access, accidental loss, or destruction
  - Data Privacy – proper handling of sensitive data
  - Data Protection – Threat identification and mitigation
- IP Packet Inspection
  - Encrypted Inspection – decryption, re-encryption, and bypass
  - Unencrypted Inspection

Use cases are included in this document to illustrate how these use cases can be addressed using Security Functions from MEF 138 [7].

The document discusses SSE and the Security Functions and Security Solutions, shown below, that are used to construct an SSE Framework:

- Proxy
- CASB
- DLP
- SG
- MEF 138 [7] Security Functions

The document describes Secure Public Access and Secure Private Access and how Secure Access Policies are used to restrict access to the SSE and to Target Actors.

The document describes how an SSE Framework contains a Proxy function, either in the Full, Forward, or Reverse direction. The Proxy function resides in one of the other functions with the SSE Framework such as the CASB or SG and acts as a Full, Forward and Reverse Proxy.

The document describes Security Solutions for CASB. These include Identity Management for supported applications, Full, Reverse, and Forward Proxy, and Data Integrity.

The document describes the portions of MEF 138 [7] that apply to DLP.

The document describes SG and its associated Security Functions including Proxy, IP, Port, and Protocol Filtering, URL Filtering, Domain Name Filtering, and Protective DNS. The SG also includes the SSE Interface Termination (defined within the document as a termination point such as an SSE UNI or SSE NNI).

Finally, the document describes how the Security Functions from MEF 138 [7] enable the SSE Framework.

7 SSE Framework Items

There are several SSE Framework items that are referenced throughout the document. Some of these are defined within this document and others are defined in MEF 138 [7], Mplify 117.1 [5], or MEF 118.1 [6]. SSE Framework item(s) can be used as stand-alone entities or combined into a set to create the SSE Framework.

The combination of the required SSE Framework items that make up the SSE Framework are defined in section 9.

7.1 Proxy

The Proxy acts as termination or origination point for the IP packets that flow between the Subject Actor and Target Actor and creates a different session from the Proxy to the Target Actor. This functionality differs from the Middlebox Security Function (MBSF) in that the Proxy terminates the sessions and the MBSF does not. The Proxy is capable of decrypting and encrypting the IP packets that are terminated and originated at the Proxy. The Proxy typically obfuscates the originating IP address of a Subject Actor. The Target Actor would thus see the Proxy as the Subject Actor for all connections. This provides inherent security benefits as the Subject Actor may or may not require to have an IP address or a direct IP routed connectivity to the Target Actor's network. A Proxy may be Forward, Reverse, or Full. Definitions of these capabilities are included in section 9.2.

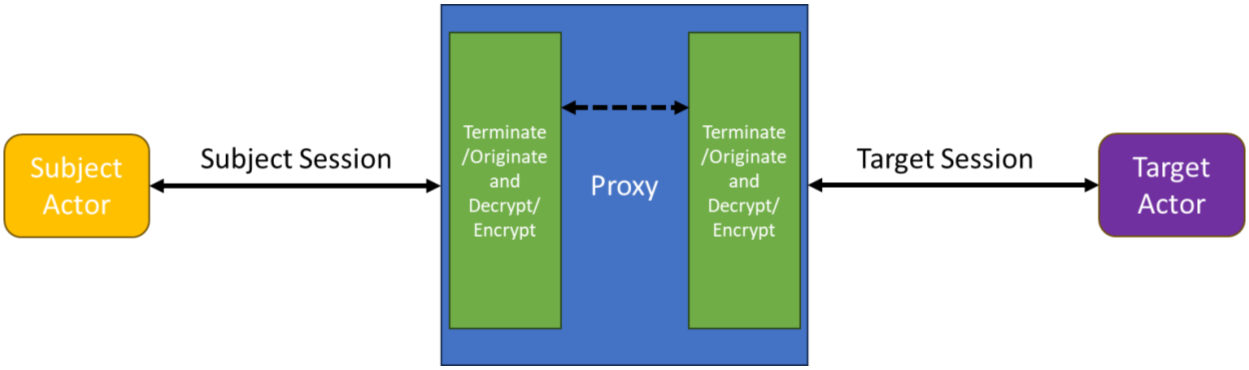
Subject Actor
Subject Session
Terminate /Originate and Decrypt/ Encrypt
Proxy
Terminate /Originate and Decrypt/ Encrypt
Target Session
Target Actor

Figure 1 – Example Proxy Functionality

7.2 SSE Interface

An SSE Interface is a logical construct within the SSE where IP packets ingress and egress the SSE. There are two types of SSE Interfaces, SSE Network to Network Interface (NNI) and SSE User Network Interface (UNI). These are defined in the following sections.

7.2.1 SSE NNI

An SSE NNI provides a point of demarcation between two entities connected over the SSE NNI and is used to interconnect the SSE to other SASE functionalities, (e.g. Zero Trust, or SD-WAN). The term NNI used throughout this document means an SSE NNI.

7.2.2 SSE UNI

An SSE UNI provides a point of demarcation between the Subscriber and the SSE SP and is used to connect a SSE Subscriber (a Subscriber who is using an SSE) to the SSE. There are no intermediate functionalities between the SSE and the Subscriber. The term UNI used throughout this document means an SSE UNI.

7.3 IP, Port, and Protocol Filtering

Per MEF 138 [7], IP, Port, and Protocol Filtering is defined as “the Security Function that determines whether a Service Flow’s source or destination IP addresses, source or destination port numbers, or IP protocols are to be Allowed or Blocked. A Security Policy might disallow specific IP addresses, IP protocols and/or port numbers that are not used by the Subscriber, to mitigate possible attacks.” IP, Port, and Protocol Filtering can, as an implementation option, also include a stateless firewall. URL Filtering, Domain Name Filtering, and DNS Filtering are additional components found in stateful and next generation firewalls.

7.4 URL Filtering

Per MEF 138 [7], URL Filtering is defined as “the Security Function that determines whether a Service Flow, or subset of a Service Flow, contains a URL that is to be Allowed or Blocked.”

7.5 Domain Name Filtering

Per MEF 138 [7], Domain Name Filtering is defined as “the Security Function that determines whether a Service Flow, or subset of a Service Flow, contains domain names that are to be Allowed or Blocked.”

7.6 DNS Protocol Filtering

Per MEF 138 [7], DNS Protocol Filtering is defined as “the Security Function that determines whether a Service Flow, or subset of a Service Flow, contains Domain Name System (DNS) messages that are to be Allowed or Blocked.”

7.7 Protective DNS

Per MEF 138 [7], Protective DNS is defined as “the Security Function that analyzes DNS queries and takes action to mitigate threats, leveraging the existing DNS protocol and architecture.”

7.8 SSE Policy End Point

The SSE Policy End Point where an SSE Policy is identified, applied, or enforced. The SSE Policy End Point is located somewhere within the SSE solution. Each SSE service offering will determine the location and the number of the SSE Policy End Points; this is beyond the scope of this document as indicated previously

7.9 Malware Detection and Removal

Per MEF 138 [7], Malware Detection and Removal is defined as "the Security Function that determines whether a Service Flow, or subset of a Service Flow, contains Malware, and removes the Malware or Blocks the subset of the Service Flow containing the Malware".

7.10 Middlebox Security Function

Per MEF 138 [7], Middlebox Security Function is defined as "a function used to decrypt and re-encrypt secured sessions, e.g., IPsec or TLS, in a Service Flow that allows other Security Functions to apply to the unencrypted Service Flow".

7.11 Data Loss Prevention

Per MEF 138 [7], Data Loss Prevention is defined as "a Security Function that determines whether a Service Flow, or subset of a Service Flow, contains confidential, sensitive, or important data, and prevents such data from being exfiltrated by people or systems either intentionally or unintentionally".

7.12 Security Event Notification

Per MEF 138 [7], Security Event Notification is defined as "a communication to the agreed upon list of Subscriber personnel of a Security Event".

7.13 Security Admin Notification

Per MEF 138 [7], Security Admin Notification is defined as "a notification to the agreed upon list of Subscriber personnel of a change to a Security Function Policy".

7.14 Identify Management

Identity Management (IdM) is defined as a function that is used by an SSE Service that adopts this SSE Framework to identify and Authenticate the Subject Actor (and possibly the Target Actor) for which Policies are applied. This definition is adapted from the definition in MEF 118.1 [6].

7.15 Supported Application Identity and Access Management

Per Mplify 117.1 [5], Supported Application Identity and Access Management is defined as "a Security Function that determines whether a Subject Actor of a Session is authenticated and authorized to access a particular supported application.” For this document, a Session is equal to a sequence of IP packets, either in or out of order, from the Subject Actor on which a specific security action is determined by the SSE Policies.

Mplify 117.1 [5] also describes a use case for SA-IdAM as “ A typical Cloud workload use case is where the Subscriber would like to control access to a particular supported application (e.g., Office365^{TM}, Salesforce^{TM}, G-Suite^{TM}, etc.). As an example, the SA-IdAM Security Function could block access to the data for individuals that do not have proper access within that supported application.”

7.16 Data Integrity

Per Mplify 117.1 [5], Data Integrity is defined as a function that “examines Sessions to certain supported applications and determines if the actions included in those Sessions are allowed or blocked.”

8 SSE Use Cases and Associated Security Functions

This document describes the following use cases:

- Secure Access – section 8.1
- Safeguarding Data – section 8.2
- IP Packet Inspection – section 8.3

8.1 Secure Access

Secure Access use cases address the Actors' controlled access via Policies. Secure Access comes in two types, Secure Private Access and Secure Public Access, as described below.

8.1.1 Secure Private Access

Secure Private Access limits access of Subject Actors to Target Actors in the Subscriber Network. Subscriber Network is defined within this document as a set of connections, functions and solutions that make up the Subscribers data service. Limiting access is done via the use of Policies.

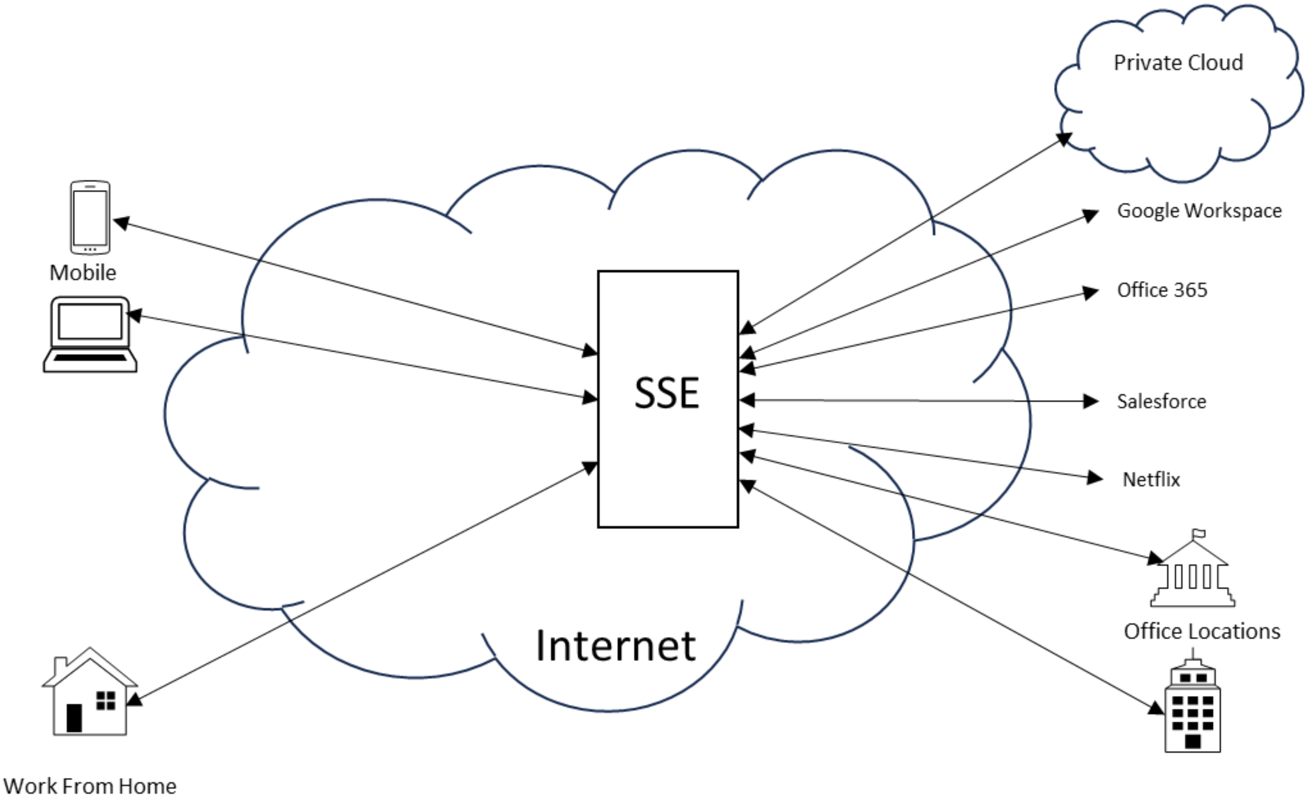

Figure 2 – Example Secure Private Access Over Internet Use Case

As shown in Figure 2 the SSE limits the access of different Subject Actors, (e.g. mobile and Work From Home (WFH)) using the Internet for access to applications on the Subscriber Network (branches, datacenters, headquarters, or private cloud instances). The Subject and Target Actors are connected to the SSE via UNIs. For example, the WFH Subject Actors may be given access to all of these Target Actors on the Subscriber network while the mobile Subject Actors can be limited perhaps to Salesforce™ but not the others. Policies are created that include the rules used to limit access of a Subject Actor.

Secure Private Access can also be utilized to limit access of Subject Actors on the Subscriber Network at a particular location from accessing Target Actors at a different location within the Subscriber Network over Private network. The SSE might have a direct connection between the SSE and the private cloud via a private network.

Subject Actor connection is controlled via one of the following:

Proxy – This is a browser proxy for the Subject Actor to access the Target Actors via Secure Private Access.

Device agent - Either Browser redirection based, or client browser based.

Secure tunnel – this is a secure network connection between the Subject Actor and the SSE.

Target Actor connection is controlled via one of the following:

App connector – this is a connection mechanism that identifies specific applications within the Subscriber Network which can be accessed via Secure Private Access.

Secure Tunnel – this is a secure network connection between the SSE and the Subscriber Network over which certain IP routes are advertised for access via Secure Private Access.

[R1] The Subject and Target Actors **MUST** be authenticated as specified in MEF 118.1 [6] section 8.

[R2] If the Subject and Target Actors are authenticated, then the Subject and Target Actors **MUST** be authorized as specified in MEF 118.1 [6] section 8.

[R3] If the Subject and Target Actors have been authenticated, then the Subject and Target Actors **MUST** be monitored as specified in MEF 118.1 [6] section 18.

8.1.2 Secure Public Access

Secure Public Access limits access of Target Actors on the Internet. Limiting access is done via the use of Policies.

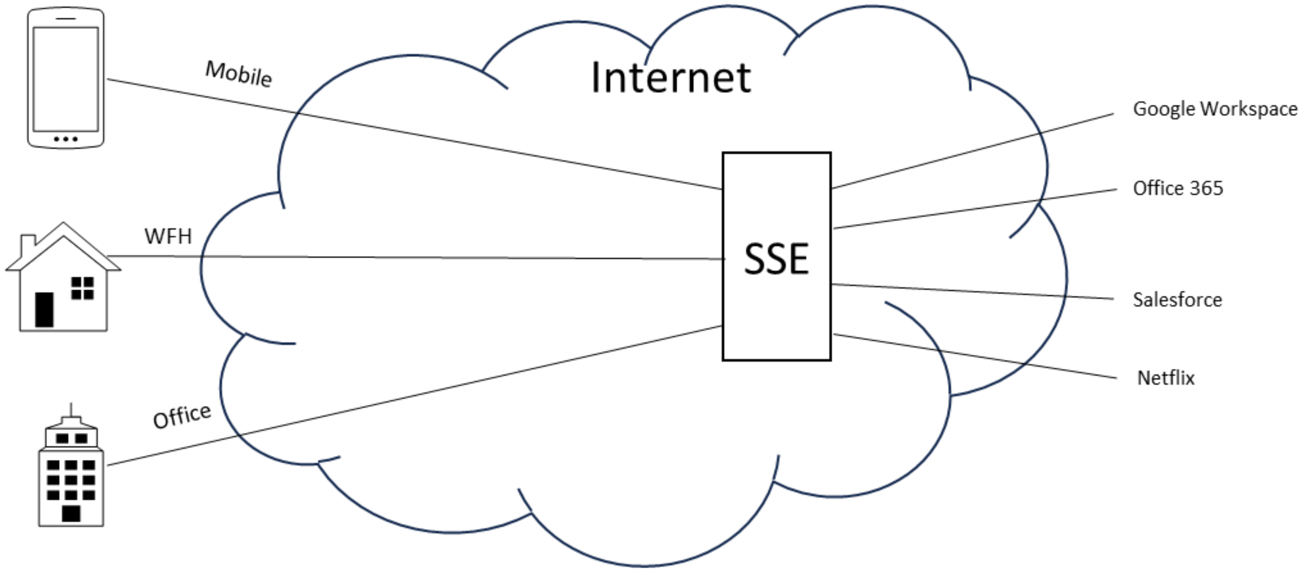

Figure 3 – Example Secure Public Access Use Case

As shown in Figure 3, the SSE shown within the cloud limits the access of different Users, (mobile, Work From Home (WFH), and Actors at Branch Locations) from access to Internet based applications such as Google Workspace™, Office 365™, Salesforce™, and Netsuite™. The Users and Actors are connected to the SSE via UNIs. For example, a Branch Office on premises based User may be given access to all of these Target applications while the access of a WFH or mobile User can be limited perhaps to Salesforce™ but not the others. Policies are created that set the rules used to limit access of a Subject Actor.

The Secure Public Access use case illustrates how to secure Internet access from a particular set of locations and prevent malicious content from being sent to/from that location. Each Secure Public Access, for a given Subject Actor at a given location, is uniquely contained and does not share information with Subject Actors at another location. Policies can be implemented that limit what Target Actors Subject Actors are able to access. As in Figure 3, each Subject Actor on the left only has access to Target Actors on the right (Internet). In essence, this is a secure Internet proxy implementation with security functionality.

Subject Actor connection is controlled via one of the following:

Web proxy – This is a browser proxy for the Subject Actor to access the Target Actors via Secure Public Access.

Device agent - Either Browser redirection based, or client browser based control.

Secure Tunnel – this is a secure network connection between the Subject Actor and the SSE.

Identity and Access Management for the Subject Actors must be completed and monitored.

When the Target Actor is in the public domain, neither the Subscriber nor the Service Provider has direct control of the Target Actor. In this case, the ability to authenticate the Target Actor might be limited. Since the ability to authenticate the Target Actor is limited, the SSE provides the Subscriber with the ability to define an SSE Policy that determines whether to authenticate Target Actors and the action to perform if authentication fails or if the Target Actor cannot be authenticated.

8.2 Safeguarding Data

Safeguarding Data is defined in this document as a method of using Security Functions to protect data. There are three distinct areas that cover safeguarding data, these are Data Security, Data Protection, and Data Privacy. These are discussed below.

8.2.1 Data Security

Data Security is a process by which the Subscriber's data is protected by Security Functions and Security Solutions such that it cannot be intercepted and disclosed by unauthorized Actors, that it is transmitted to only appropriate Actors, and that all of this is controlled by SSE Policy. Data Security may be provided by one or more different Security Solutions or Functions. These are CASB, DLP, and SG. While they are similar to each other, each of these Security Solutions or Functions provide unique capabilities.

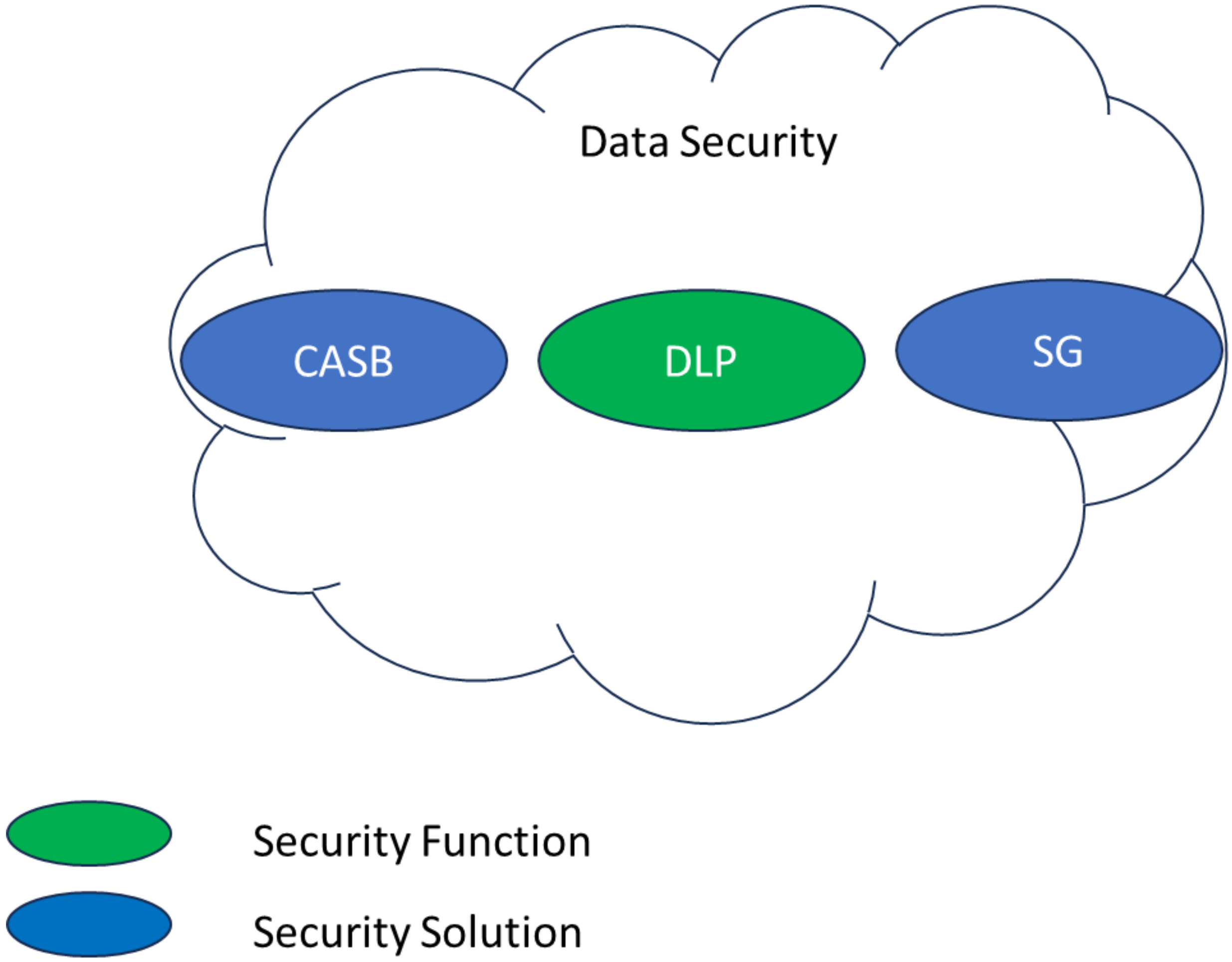

Figure 4 – Example Data Security Use Cases

The two Security Solutions and the Security Function are described in the following sections.

8.2.1.1 Cloud Access Security Broker

The CASB Security Solution covers the following areas of Data Security:

- Supported identity and access management for SaaS/IaaS
    - Authenticate a Subject Actor to access a specific cloud application (Target Actor)
    - Authorize a Subject Actor to access a specific cloud application (Target Actor)
- Proxy
    - Forward
    - Reverse
    - Full

- Data Integrity Action
  - Store
  - Upload
  - Download

8.2.1.2 Data Loss Prevention

The use case for DLP is defined as verifying that data cannot be exfiltrated by others. Section 9.5 of MEF 138 [7] provides additional information on this use case.

8.2.1.3 Secure Gateway

The SG Security Solution provides a method that prevents access to data without the correct permissions contained within applicable SSE Policies. SG uses the following functions:

- Proxy
- SSE Interface
- IP, Port, and Protocol Filtering
- URL Filtering
- Domain Name Filtering
- Protective DNS

Additionally, the SG firewall function may allow for the use of other application (Target) attributes such as Fully Qualified Domain Name or URL.

Mplify has decided to use the term Secure Gateway to represent marketing terms such as Secure Web Gateway (SWG) or Private Gateway. Secure Web Gateways have evolved to deal with more than just HTTP/HTTPS traffic, and as such are no longer just concerned with "Web" traffic. SWGs are often referred to as a security function that only arbitrates access for Internet based traffic. However, nothing prevents these SWGs from being utilized for use cases that do not involve the Internet. For example, a SWG could be utilized to protect web applications in a private cloud instance that does not use internet as an access medium. For this reason, Mplify uses the term Secure Gateway which does not infer a particular use case but rather a specific set of functions.

8.2.2 Data Privacy

Data Privacy is a process by which the Subscriber's data is protected by Security Functions and Security Solutions such that it is transmitted to only appropriate Actors, contains only the appropriate information allowed to be shared with given Actor, and that all of this is controlled by SSE Policy. Data Privacy requires the following Security Solutions and Functions:

- CASB - Solution
- DLP - Function
- SG - Solution

CASB, and SG are Security Solutions, and DLP is a Security Function that can be used to limit access to sensitive data only to those who are authorized to access it. Sensitive data can include Subscriber data (individuals) and company data (corporate data). See sections 9.3, 9.4, and 9.5 for detailed descriptions of these topics.

8.2.3 Data Protection

Data Protection is the process by which the Subscriber Data is protected from malicious threat injection, compromise, or infiltration and is controlled by SSE Policy. Data protection uses several Security Functions to identify and mitigate threats to the security of the data, e.g. unauthorized access to the data, corruption of the data, inserting malware into the data, etc. CASB using Out of Band identification and mitigation is one Security Solution that can provide data protection. Another Security Solution that can provide data protection is Firewall as a Service (FWaaS) (defined as a firewall solution delivered as a cloud-based service) through the following:

- IP, Port, and Protocol filtering
- URL filtering
- Domain Name filtering
- Protective DNS
- Malware Detection and Removal

Finally, an SG may provide a Proxy function for data protection.

8.3 IP Packet Inspection

IP packet inspection covers encrypted and unencrypted packet inspection.

8.3.1 Encrypted Inspection

Inspection of encrypted packets such as Transport Layer Security (TLS) allows the SSE to decrypt IP packets, inspect the IP packets, and re-encrypt the IP packets. This inspection is described in detail in MEF 138 [7] section 8 (Middlebox Function).

8.3.2 Unencrypted Inspection

Inspection of unencrypted IP Packets allows the SSE to inspect IP packets as described in detail in MEF 138 [7] section 8 (Middlebox Function).

9 SSE Framework

An SSE Framework contains different Security Solutions and Functions that interact with each other to provide an SSE. An SSE Framework contains the following Security Solutions and Functions:

- Security Solutions
  - Secure Access
  - CASB
  - SG
- Security Functions
  - IP, Port, and Protocol Filtering
  - URL Filtering
  - Domain Name Filtering
  - DNS Protocol Filtering
  - Malware Detection and Removal
  - Middlebox Security
  - DLP
  - Security Event Notification
  - Security Admin Notification
  - Identify Management
  - Supported Applications
  - Data Integrity
  - Proxy

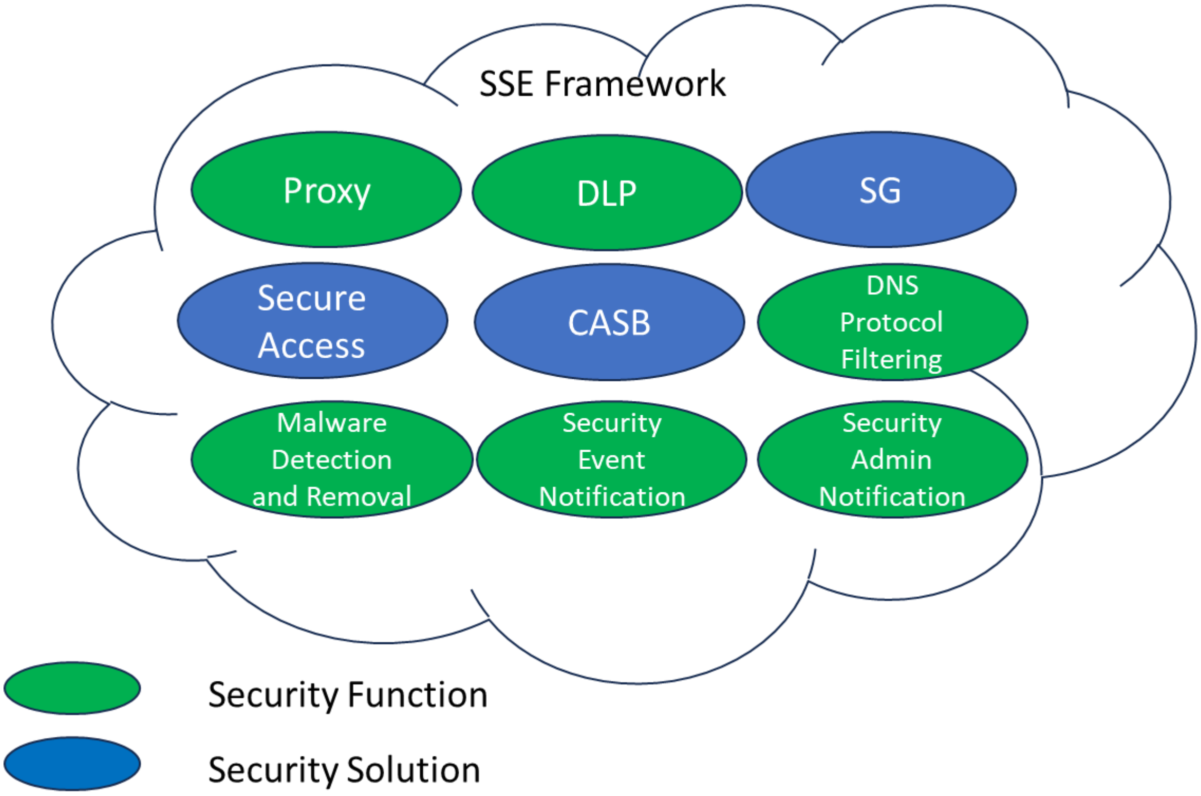

Figure 5 – High-Level SSE Framework

Figure 5 shows a high-level view of an SSE Framework. The SSE Framework is made up of the three Security Solutions and six Security Functions shown above. Each of these are discussed below.

[R4] An SSE Solution that is compliant with this SSE Framework **MUST** support all of the Security Solutions and Security Functions discussed in this document.

9.1 Secure Access

Secure Access is defined within this document as the ability to restrict Subject Actors from accessing Target Actors using one or more Policies or rules. It is applicable to both Private and Public access.

Zero Trust authenticates an Actor and provides them access to other Actors. SSE Secure Access takes this a step further by applying additional contextual Policy parameters to determine if an Actor has the authority to access specific Actors. This can include the authority to access items like specific documents managed by an Actor or access to specific domains managed by an Actor.

Identity Management is included in Secure Access. Verification of identity allows the correct access to Target Actors to be performed.

The requirements for the Secure Access Security Solution are defined below.

[R5] A Subject Actor **MUST** be authenticated as specified in MEF 118.1 [6] section 8.3.

[D1] A Target Actor **SHOULD** be authenticated as specified in MEF 118.1 [6] section 8.3.

[R6] If the Subject and Target Actors are authenticated, then the Subject and Target Actors **MUST** be authorized as specified in MEF 118.1 [6] section 11.

[R7] If the Subject and Target Actors have been authenticated, then the Subject and Target Actors **MUST** be monitored as specified in MEF 118.1 [6] section 18.

[D2] If a Target Actor has not been authenticated, then the Target Actor **SHOULD** be monitored as specified in MEF 118.1 [6] section 18.

[R8] Secure Access Policies or rules **MUST** define which Subject Actors can access which Target Actors and which specific items (or domains) that are managed by the authorized Actors.

9.2 Proxy

A Proxy is defined within this document as a Security Function that terminates/originates a flow from a Subject Actor and terminates/originates a flow from a Target Actor. The Proxy may encrypt and decrypt parts of the flow.

The Proxy function works in the Forward, Reverse, and Full (both Forward and Reverse) directions. A Forward Proxy is defined as a Security Function that:

- terminates the Subject Actor’s session to a given Target Actor
- initiates a new session on behalf of the Subject Actor to the Target Actor
- masks the Subject Actor from the Target Actor
- protect the Subject Actor from malicious traffic from the Target Actor
- limit the data/transaction sent from the Subject Actor to the Target Actor

In a Forward Proxy, the Subject Actor’s session is terminated and a new session initiated to mask the Subject Actor from the Target Actor. Additionally, Security Policies can be applied at the Proxy level to protect the Subject Actor from malicious traffic returned by the Target Actor and limit what the Subject Actor can send to the Target Actor. An enterprise’s use of an internet proxy is a widely known example of a Forward Proxy.

A Reverse Proxy is defined as a Security Function that:

- terminates the Subject Actor’s session to a given Target Actor

- initiates a new session on behalf of the Subject Actor to the Target Actor
- restricts the Subject Actor access to the Target Actor
- protect the Target Actor from malicious traffic from the Subject Actor
- limit the data/transaction exchanged between the Subject Actor and the Target Actor

In a Reverse Proxy, the Subject Actor's session is terminated and a new session initiated to the Target Actor. Additionally, Security Policies can be applied at the Proxy level to protect the Target Actor from malicious traffic sent by the Subject Actor and limit what data and transactions can be exchanged between the Target Actor and the Subject Actor. For example, there are SaaS applications (e.g. email server) on the Internet that need to access devices internal to the enterprise network (enterprise email server). Enterprises rarely want their email servers directly connected to the internet. The Reverse Proxy is used to limit the SaaS email application access to the internal email server.

A Full Proxy has the capability of performing both Forward and Reverse Proxy functionality.

[R9] An SSE Framework **MUST** support the Forward Proxy functions.

[R10] An SSE Framework **MUST** support the Reverse Proxy functions.

[D3] An SSE Framework **SHOULD** support the Full Proxy functions.

A Full Proxy can be provided by having separate Forward and Reverse Proxy implementations.

9.3 Cloud Access Security Broker

CASB is defined within this document as a solution that performs Identity Management for Software as a Service and Infrastructure as a Service and CASB Action. Identity Management is defined as a framework of Policies and technologies to ensure that the right users have the appropriate access to technology resources.

In addition to Identity Management, CASB also manages Proxies or Middle Box Security Functions and Actions such as Store, Upload, and Download.

9.3.1 Application Identity and Access Management

Application Identity and Access Management is defined as a Framework of Policies and technologies to ensure that the right Actors have the appropriate access to technology resources.

[R11] An Application Identity and Access Management function within a CASB solution **MUST** support all the Mandatory requirements defined in MEF 118.1 [6] section 8.

9.3.2 Proxy or Middle Box Security

The Proxy or Middle Box Security Function protects clients and file servers from threats.

[R12] A CASB solution **MUST** contain a Proxy or a Middle Box Security Function.

[R13] If a CASB is deploying a Middle Box Security Function rather than a Proxy, it **MUST** be as defined in MEF 138 [7] section 8.

9.3.3 CASB Action

There are multiple CASB Actions that can be supported by CASB. The CASB Actions supported depend on the application. As an example, for a storage solution, the CASB Actions Store, Upload, and Download may be supported while for an API solution GET, POST, and MODIFY may be the CASB Actions supported.

[R14] A CASB Security Solution **MUST** support the CASB Action Function.

The specific CASB Actions supported are beyond the scope of this document.

9.4 DLP

DLP is defined in MEF 138 [7] as "a Security Function that determines whether a Service Flow, or subset of a Service Flow, contains confidential, sensitive, or important data, and prevents such data from being exfiltrated by people or systems either intentionally or unintentionally. This Security Function does not cover the case where the Subscriber no longer has access to the data."

The following requirements apply for SSE Framework.

[R15] An SSE Framework **MUST** support all mandatory requirements for DLP in MEF 138 [7] section 9.5.

9.5 Secure Gateway

The Secure Gateway Security Solution, in this document, is meant to represent marketing terms such as Secure Web Gateway (SWG) or Private Gateway. The Mplify SG Security Solution is used to protect both Internet and private web applications. SG is defined within this document as a minimum set of SSE Framework Items that make up an SG Security Solution. These functions are:

- Proxy
- SSE Interface
- IP, Port, and Protocol Filtering
- URL filtering

- Domain Name Filtering
- Protective DNS

The requirements for each SSE Functional Item that make up a Secure Gateway are defined in the following sections.

9.5.1 Proxy

For requirements for the Proxy functionality see section 9.2.

9.5.2 SSE Interface

An SSE Interface allows the traffic to ingress to and to egress from the SSE Framework; the SSE Framework has at least one SEE Interface ([R16]). The SSE can have multiple SSE Interfaces.

[R16] An SSE Framework **MUST** have at least one SSE Interface.

[R17] If an SSE Interface uses an Ethernet physical layer, it **MUST** support an external interface of Ethernet as described in MEF 61.1.1 [4].

[R18] An SSE Interface **MUST** provide a way for traffic destined for the SSE Framework to ingress the SSE Framework.

[R19] An SSE Interface **MUST** provide a way for the traffic sent by the SSE Framework to egress the SSE Framework.

[R20] An SSE Interface connecting to other SASE components (i.e. SD-WAN and Zero Trust) **MUST** be an SSE NNI.

[R21] An SSE Interface connecting to Subscribers **MUST** be an SSE UNI.

9.5.3 IP, Port, and Protocol Filtering

IP, Port, and Protocol Filtering is described in MEF 138 [7].

[R22] The Secure Gateway solution **MUST** support IP, Port, and Protocol Filtering as defined in MEF 138 [7].

9.5.4 URL Filtering

URL Filtering is described in MEF 138 [7].

[R23] The Secure Gateway solution **MUST** support URL Filtering as defined in MEF 138 [7].

9.5.5 Domain Name Filtering

Domain Name Filtering is described in MEF 138 [7].

[R24] The Secure Gateway solution **MUST** support Domain Name Filtering as defined in MEF 138 [7].

9.5.6 Protective DNS

Protective DNS is described in MEF 138 [7].

[R25] The Secure Gateway solution **MUST** support Protective DNS as defined in MEF 138 [7].

9.6 DNS Protocol Filtering

DNS Protocol Filtering is defined in MEF 138 [7].

[R26] An SSE Framework **MUST** support DNS Protocol Filtering as specified in MEF 138 [7].

9.7 Malware Detection and Removal

Malware Detection and Removal is defined in MEF 138 [7].

[R27] An SSE Framework **MUST** support Malware Detection and Removal as defined in MEF 138 [7].

9.8 Security Event Notification

Security Event Notification (SEN) is defined in MEF 138.

[R28] An SSE Framework **MUST** support Security Event Notification as defined in MEF 138 [7].

9.9 Security Admin Notification

Security Admin Notification (SAN) is defined in MEF 138 [7].

[R29] An SSE Framework **MUST** support Security Admin Notification as defined in MEF 138 [7].

10 SSE Policy

SSE Policies are defined as the instructions for SSE operation within this document. The requirements for Policies that support the SSE Framework are included within this section of the document. These Policies are defined per area of the framework. All Policies are applied to IP Packets within an SSE service flow. The definition of an SSE service flow is beyond the scope of this framework document.

10.1 Secure Access Policies

The requirements for Secure Access Policies are defined below.

[R30] The Secure Access Policies **MUST** provide the ability to define what Target Actors a Subject Actor is able to access.

10.2 Proxy Policies

The requirements for Proxy Policies are defined below.

[R31] The Proxy Policies **MUST** provide the ability to define the behavior of a Forward Proxy.

[R32] The Proxy Policies **MUST** provide the ability to define the behavior of a Reverse Proxy.

[CR1]<[D3] The Proxy Policies **MUST** provide the ability to define the behavior of a Full Proxy.

10.3 Cloud Access Security Broker Policies

The requirements for CASB Policies are defined below.

[R33] The CASB Policies **MUST** provide the ability to define the behavior for CASB Security Solution.

10.4 Data Loss Prevention Policies

The requirements for DLP Policies are defined below.

[R34] DLP Policies **MUST** provide the ability to define the behavior of DLP as defined in MEF 138 [7].

10.5 Secure Gateway Policies

The requirements for Secure Gateway Policies are defined below.

[R35] The Secure Gateway Policies **MUST** provide the ability to define the behavior for Secure Gateway Security Solution.

Note: Secure Gateway Security solution includes Forward and Reverse Proxy, IP, Port, and Protocol Filtering, URL Filtering, Domain Name Filtering, and Protective DNS actions as defined in section 9.5.

10.6 DNS Protocol Filtering Policies

The requirements for DNS Protocol Filtering Policies are defined below.

[R36] The DNS Protocol Filtering Policies **MUST** provide the ability to define DNS Protocol Filtering actions as defined in MEF 138 [7].

10.7 Malware Detection Policies

The Malware Detection Policies are defined below.

[R37] The Malware Detection Policies **MUST** provide the ability to define, detect, and act upon Malware as defined in MEF 138 [7].

Note: “act upon” Malware might include actions such as logging, quarantining, or removing as defined in MEF 138 [7].

10.8 Security Event Notification Policies

The Security Event Notification Policies are defined below.

[R38] The Security Event Notification Policies **MUST** provide the ability to define Security Event Notifications as defined in MEF 138 [7].

10.9 Security Administrator Notification Policies

The Security Administrator Notification Policies are defined below.

[R39] The Security Administrator Notification Policies **MUST** provide the ability to define Security Administrator Notification actions as defined in MEF 138 [7].

11 References

[1] Gartner, Zero Trust Network Access Reviews and Ratings, https://www.gartner.com/reviews/market/zero-trust-network-access

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

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

[4] MEF 61.1.1, Amendment to MEF 61.1: UNI Access Link Trunks, IP Addresses, and Mean Time to Repair Performance Metric, July 2022

[5] Mplify 117.1, SASE Service Attributes and Service Framework Revision, June 2025

[6] MEF 118.1, Zero Trust Framework for MEF Services, July 2024

[7] MEF 138, Security Functions for IP Services, July 2024

Appendix A Zero Trust Network Access (Informative)

Mplify loosely defines Zero Trust Network Access (ZTNA) as access from any Subject Actor at any location, any time, and under any circumstance to any Target Actor at any location, any time, and under any circumstance. In ZTNA, based on defined access control (defined as a security technique that regulates who or what can view or use resources in a computing environment) Policies, its identity aware proxy design uses least privilege principles and contextual insights to granularly deny access by default and brokers user access to applications when explicitly granted, irrespective of location. Just as the name implies, there is no network access by anyone or anything at any time, any location, or under any circumstance unless a specific Policy allows said access and after identity and context are verified access is granted . Even then, this access is granted with the least privilege needed to accomplish the access. This access is also continuously monitored for compliance with the Policy.

This definition of ZTNA differs from the industry generally accepted definition. Gartner defines Zero Trust Network Access (ZTNA) [1] as “products and services that create an identity and context-based, logical-access boundary that encompasses an enterprise user and an internally hosted application or set of applications.” In the Gartner definition, ZTNA has become synonymous with the remote access or VPN replacement model. However, this Gartner definition ignores the on-premises use case of Zero Trust Network Access and access to Target resources located on the Internet or externally hosted. Mplify includes all aspects of access in its definition of ZTNA. The network term utilized in the Mplify ZTNA definition does not refer to any specific network (e.g., access network, Service Provider network, Subscriber network, core network, cloud network, or any virtualized network). This Mplify definition of ZTNA considers all access between any Actor to any other Actor as subject to Zero Trust Policies.

Secure Public Access (including the Mplify defined ZTNA) is focused on securing Internet access where Gartner’s definition of ZTNA focuses only on access to internally hosted enterprise applications.

Appendix B Acknowledgements (Informative)

The following contributors participated in the development of this document and have requested to be included in this list.

- Mike **BENCHECK**
- Richard **CARRARA**
- Neil **DANILOWICZ**
- Charles **ECKEL**
- Abhishek **KUMAR**
- Samaresh **NAIR**
- Basil **NAJIM**