MEF White Paper

MEF SASE Services Framework

July 2020

Disclaimer

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

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

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

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

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

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

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

Table of Contents

List of Figures

List of Tables

1 Abstract

This White Paper is aimed at both enterprises that are increasingly depending on digital services serving users in increasing numbers, types and locations, as well as the service providers that want to offer them security for those digital services. The paper builds upon the concept of converged networking and security described by Gartner in SASE. It proposes and describes the outline of a framework for SASE Services which could be standardized in MEF based on existing standardization work for SD-WAN services (MEF 70.x) and Application Security (MEF W88), and other related MEF work.

2 Introduction

Networking and security are converging. It is no longer possible to manage and coordinate multiple silos of security and networking effectively within the enterprise or the service provider. Gartner made a very effective start in describing this convergence and its importance with their SASE (Secure Access Service Edge) report[1]. Since then, a range of innovative SASE-oriented solutions have emerged but, as with any new technology-based market, the ecosystem stakeholders are having to invent their own descriptions and terminologies. This quickly leads to market fragmentation and confusion, holding back growth of the market and innovation – to everyone's detriment.

MEF has a successful track record in defining the standardized abstract constructs, attributes and architectures for data connectivity services such as Carrier Ethernet and more recently, SD-WAN. By achieving consensus on what an abstracted converged software-defined networking and security framework, and services, should look like, technology and service providers can then focus their efforts on innovation and solutions rather than educating the market on their own particular set of terminologies.

Work underpinning this type of consensus is already well underway in MEF. MEF W88 is defining abstracted security functions that will be deployed in a proposed SASE service – effectively the security aspect of a standardized SASE Service. It should be noted that MEF W88 has already

[1] https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

introduced standardization of Middle Box Function, a security function referenced as being important to address in the Gartner paper. MEF W70.1 builds upon the established standard MEF 70 (SD-WAN attributes and service definition) published in 2019 introducing the concept of 'zones' that will be important for operating security in a SASE context. MEF 70 itself already provides the abstract definitions for the networking aspect of SASE. MEF's Policy Driven Orchestration work provides the underpinnings for end-to-end SASE service policy management. Similarly, new work has been initiated in MEF to address Zero Trust Networking for an identity-based paradigm that is an essential component for SASE Services.

In this document, service provider and technology provider members of MEF – several of whom are already offering SASE-oriented solutions - build upon the existing MEF work in software defined networking, security and policies described above to propose the outline of such standardization of abstracted SASE services.

3 SASE Services

This paper proposes a new construct called 'SASE Service' which is defined as *"A service connecting users (machine or human) with their applications in the cloud while providing connectivity performance and security assurance determined by policies set by the Subscriber."* SASE Services will provide the optimal combination of networking and security performance for a given subscriber by distributing networking and security functionalities dynamically along the SASE Service path based on subscriber-managed policies.

Figure 1: SASE Service

The proposed abstract constructs in this section collectively describe an overall standardized converged networking/security/policy framework that can be used by service providers and enterprises alike to transform their consumption of applications in the cloud in the form of such SASE Services.

Figure 1 shows a SASE Service as a combination of two service endpoints, networking functions, and security functions. The table below lists examples of networking functions and security functions in a SASE Service. Note that the list is far from exhaustive.

Subscriber Endpoints	Networking Functions	Security Functions	Service Endpoints
Defined by Identity+Context	Routing	Firewall	Internet Sites (e.g. Twitter, Facebook)
	Path Selection	Threat prevention/detection	SaaS apps and APIs (e.g. SalesForce, O365)
	QoS	Cloud app discovery	IaaS/PaaS (e.g. AWS, Azure)
	VPN	UEBA/fraud	My apps and APIs on premises
	Cost optimization	DNS protection	My apps and APIs in service provider cloud
	Bandwidth optimization	Sensitive data discovery	My apps and APIs in wholesale provider cloud
	Deduplication	Obfuscation/privacy	Partner apps and APIs
	SaaS acceleration	WAF/WAAP	Edge computing capabilities
	Traffic shaping	Remote browser isolation	
	Latency optimization	Wifi protection	
	Caching	SWG	
	CDN	DLP	
	Path resiliency	SDP/ZTNA	
	Redundancy	Network encryption/decryption	
	Geo restrictions	CASB	

Table 1 – Example Networking and Security Functions, as well as Service Endpoints

3.1 SASE Service Stakeholders

The **SASE Subscriber** is the entity that buys and/or uses the SASE Service. Conversely, the **SASE Service Provider** is the supplier of the SASE Service that is contracted to the SASE Subscriber according to a Service Level Agreement (SLA). It should be noted that the SASE Service Provider is accountable for delivering the end-to-end SASE Service according to the SLA but that Service Provider may not have direct and full control of each component in the service (e.g. the service endpoints which may be co-managed with the subscriber enterprise; the service endpoint in the cloud may be 'operated' by a wholesale cloud provider)

3.2 Subscriber Identity and Context

The **identity** of the subscriber is the collection of persistent subscriber characteristics that don't change with time.
Examples of Subscriber Identity include:

- Name of person
- Employee ID
- MAC address of laptop
- Unique identifier of IoT device

The **context** of the subscriber is the collection of subscriber characteristics that may change with time.
Examples of Subscriber Identity include:

- Location
- Time of day
- Risk/trust assessment of the access device
- Presence (location, historical patterns)
- Authentication strength (weak, strong)
- Level of Assurance (NIST levels, X.509 certificates)
- Risk Assessment (pattern analysis)
- Federation (partner attributes)
- Device characteristics (fingerprint, device health, device protection, trusted data)
- Assertions from trusted partners (SAML tokens, etc.)
- Single Sign On sessions (session time outs)

3.3 SASE Subscriber Endpoint

A SASE Subscriber Endpoint is the point at which the SASE Service starts. It is the combination of identity and context of the SASE Subscriber Endpoint that determines if/which SASE Service is provided to a user – be it human or machine, mobile, within the campus etc. – as well as which policy to apply.

3.4 SASE Service Endpoint

A SASE Service Endpoint is the service termination point in the cloud (e.g. an application that is consumed by a subscriber via a SASE Service). The SASE Service Endpoint also has identity and context that in combination are used to determine authorization for the Subscriber Endpoint.

3.5 SASE Service Domains

Domains define the borders in the SASE Service ecosystem which a SASE Service may traverse from the SASE Subscriber Endpoint to the SASE Service Endpoint. These domain borders delineate between the entities responsible for the data flowing through the SASE Service. There are four categories of SASE Domain– Subscriber, Service Provider, Wholesale Provider and Data Center.

3.5.1 Subscriber Domain

The Subscriber Domain covers all SASE Subscriber Endpoints for which the SASE Service Subscriber or **'Subscriber'** (e.g. enterprise) is the entity that sets the Identity and Context for the Subscriber Endpoint, as well as all data compute, storage and connectivity in the path of a SASE service under the control of the Subscriber. The Subscriber Domain will often cover campuses and office buildings, remote locations including employee home offices, industrial infrastructure, as well as all user and IoT devices accessing applications from outside the enterprise campus.

3.5.2 Service Provider Domain

The Service Provider Domain covers all data compute, storage and connectivity elements on the path of a SASE service that are within the control of the Subscriber's contracted service provider supplier of data services or '**Service Provider'**. This domain includes the Service Provider Edge, Service Provider Security Cloud and the Service Provider Application Cloud (described below).

3.5.3 Wholesale Provider Domain

The Wholesale Provider Domain covers all compute, storage and connectivity elements on the path of a SASE service within the control of any contracted wholesale supplier of data services to the Subscriber's service provider. The Wholesale Provider is contracted only with the Service Provider and not the Subscriber. There are likely to be multiple cloud providers operating in this abstracted wholesale provider domain even for a single Subscriber.

3.5.4 Data Center Domain

The Data Center Domain covers all compute, storage and connectivity elements on the path of a SASE service owned by the Subscriber but controlled by a contracted third party (e.g. data center). This domain hosts the off-campus private applications of the Subscriber. The primary difference between the Service Provider/Wholesale Provider domains and the Data Center domain is that the latter is hosting private Subscriber data compute and storage that could not be achieved by the Subscriber in a different domain.

3.6 SASE Security Functions

SASE Security Functions include any security functions that may be relevant to protecting an application flow in the SASE Service and that can be layered in at any point in the SASE Service depending on the needs and authorizations of the Subscriber Endpoint and the applications.

In addition, Security Functions are being defined in MEF W88 for application flows traversing SD-WAN managed services and they currently include:

- Middle Box Function
- Security Action List Types
- Security Action List Usage Policy
- Security Event Notification
- Port and Protocol Filtering
- DNS Protocol Filtering
- Domain Name Filtering
- URL Filtering
- Malware Detection and Removal
- Data Loss Prevention
- Network Intrusion Detection and Prevention

3.7 SASE Edges

SASE Edges are the collections of compute and storage that enable a combination of networking and security capabilities along the path of the SASE Service. There are three types of SASE Edges – Subscriber, Service Provider and Data Center. SASE Edges are always mentioned in a SASE Service but they are not required for a given SASE Service to be populated with networking and/or security functionalities (i.e. they can be 'empty') although they typically do provide at the very least some networking functions.

In the case of the Subscriber Edge, the SASE Edge can, in addition to security functions, include a number of networking functions including ones which can influence how traffic is steered in the SASE Service path. These steering functions can be inline data steering functions or offline functions such as DNS proxy entries. For example, a Subscriber Edge may be a simple gateway function from a Wifi directly to an Internet access service.

Figure 2: SASE Edges

*Note: There was considerable discussion among the contributors to this paper regarding the term 'edge'. It was pointed out that 'SASE Edge' is in fact '**S**ecure **A**ccess **S**ervice **E**dge Edge' with the word 'edge' repeated. The terms 'SASE Appliance' and 'SASE Point' were considered but each one was deemed to be inappropriate for other reasons. It was decided to leave the term 'edge' since SASE will probably become a recognized enough term that it ceases to be treated as an acronym.*

3.8 SASE Security Clouds

SASE Security Clouds are the collections of compute and storage that contain security functions used to secure application flows in a SASE Service prior to accessing the SASE Service Endpoints. There are two types of SASE Security Cloud – the Service Provider Security Cloud and the Data Center Cloud. In contrast to SASE Edges, SASE Security Clouds only contain security functions (i.e. no networking functions). However, like SASE Edges, the level of security functionality can be set to zero by the SASE Service policy.

Figure 3: SASE Service Components

Figure 3 brings together all the possible components in a SASE Service. However, there will be a range of permutations depending on the SASE Service type (described later in this document). For example, in some SASE Services do not include an SD-WAN component.

3.9 Application Clouds

The Application Clouds contain the applications being accessed by the SASE Subscriber Endpoints. There are three types of Applications Clouds in the SASE Service framework – Service Provider, Wholesale and Data Center. They may contain some security functions.

3.10 SASE Service Policy

A SASE Service Policy is the set of rules and conditions relating to networking and security which are determined by the SASE Service Subscriber and that are applied to a SASE Service. SASE Service Policies are enforced throughout the path of the SASE Service so as to maximize performance and security of application flows running over the service. The SASE Service paradigm enables a consistent end-to-end approach to policy decision-making and enforcement, eliminating the current silo-type implementations that make application flows potentially vulnerable to security and performance failures.

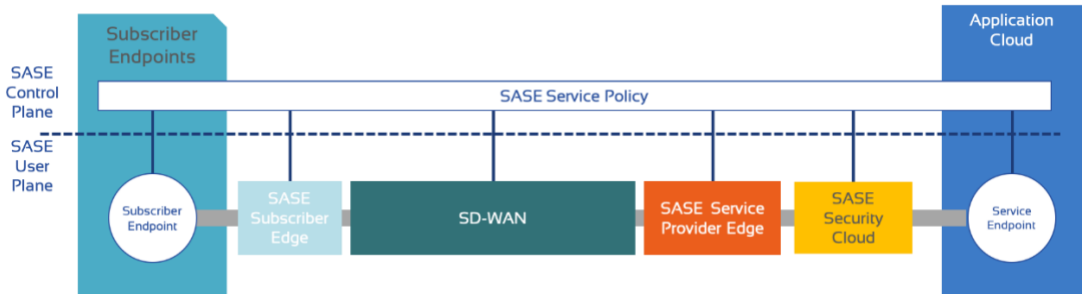

Figure 4: SASE Service Policies

3.11 SASE Service Policy Controller

A SASE Service Policy Controller is the mechanism through which the SASE Service Subscriber determines policies and how they should be enforced. Furthermore, the Controller allows the Subscriber to achieve a single-pane of glass view of the network and security performance of the SASE Service from end to end.

3.12 SASE Interface Reference Points

SASE Interface Reference Points are the abstract points in the framework at which SASE Service Policies are enforced.

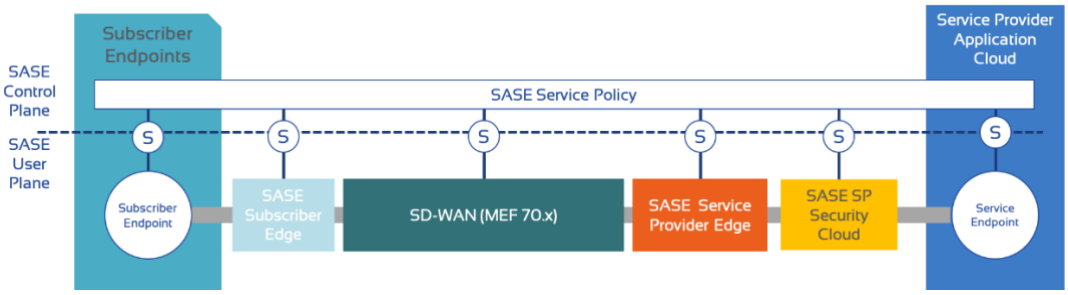

Figure 5: SASE Interface Reference Points (S in circles)

4 SASE Service Framework

Having defined SASE Services and their components, we bring them together into a single framework diagram show below in Figure 6. Although SASE was originally proposed in the context of inverting the typical approach to networking and security by making the identity of the user the focal point, in this paper we depict the user in an outer ring trying to access applications and services in the 'core'. The core of applications and services is shown as four quadrants – one for service provider cloud, one for private data center cloud, one for wholesale provider cloud and one for public internet.

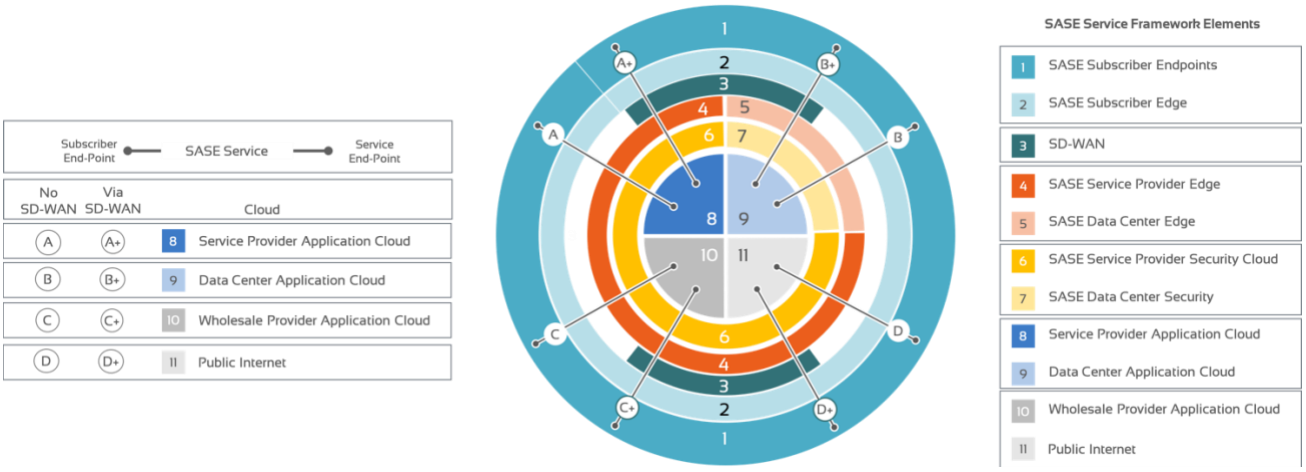

Figure 6: SASE Service Framework

The outer ring (1) is the collection of Subscriber Endpoints that need to access one or more applications in the cloud (8, 9, 10 and 11) in a secure manner with suitable performance guarantees. They cannot access the applications, all of which are located in the core of the diagram, without traversing the SASE Edges and Security Clouds. To do this, they use one of four types of SASE Service. Which type of SASE Service is used is determined by the context of the SASE Service Endpoint (i.e. which endpoint – Service Provider, Data Center, Wholesale Provider or Public Internet). Note that SD-WAN (3) is an optional element in the SASE Service.

In the following section, we describe each SASE Service type in more detail with example use cases.

4.1 SASE Service Types

In order to ease the communications between SASE Service Providers and their Subscriber customers, this paper proposes creating four SASE Service types (A-D) that each have a unique combination of SASE Service framework elements (e.g. edges, SD-WAN, cloud). The following sections provide a representative graphic and an example use case with a combination of identities/contexts, networking, security and application clouds. Those service types that include SD-WAN in the SASE Service are denoted with a '+' symbol.

In contrast to the 'top view' of SASE Services in Figure 6, all the following sections depict the SASE Service in a 'side view'. Similarly, the tables with the example functionalities are show the color-coded elements in the side view.

4.1.1 Service Type A/A+

Description: Access to Service Provider Application Cloud

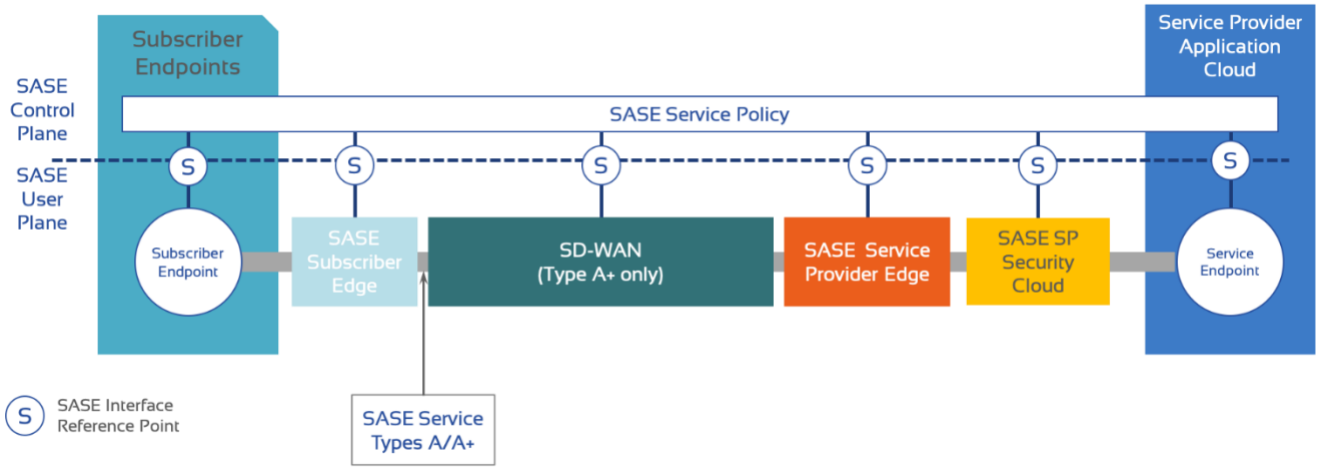

Figure 7: SASE Service Types A/A+

SASE Service Component	Subscriber Endpoint	Subscriber Edge	SD-WAN (Service Type A+ only)	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Service Provider
Example Implementation	Employee on workstation on LAN; Employee on laptop via WiFi	SD-WAN Edge	MEF 70 SD-WAN managed service	Service Provider PoP	Service Provider PoP	SAP; CRM; ERP
Example Security Functions	Embedded endpoint security	Firewall at SD-WAN Edge Encryption using IPSec and TLS	TVC encryption (optional)	No security functions	MBF; DPI; SSL Inspection; DLP; Threat Prevention	Application-level security based on identity and authorization.
Example Networking Functions		Routing and forwarding	UCS; TVC; SDWC	Routing and forwarding including segmentation	No networking functions	No embedded networking functions

Table 2 - Service Type A+ Example

SASE Service Component	Subscriber Endpoint	Subscriber Edge	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Service Provider
Example Implementation	Kiosks; Public WiFi access points	None	Service Provider Cloud	Service Provider Cloud	SAP; CRM; ERP
Example Security Functions	Basic TLS access	None	None	Single sign-on; IAM; CASB; FWaas; ZTNA/SDP; SWG; DLP; Threat protection; Sandbox; BI; CASB.	Application-level security based on identity and authorization.
Example Networking Functions	DNS or other standard mechanism to steer traffic to SASE service edge.	None	Routing; Proxy; Load balancing; Service chaining; TCP optimization; Caching; CDN	None	N/A

Table 3 - Service Type A Example

4.1.2 Service Type B/B+

Description: Access to Data Center Application Cloud

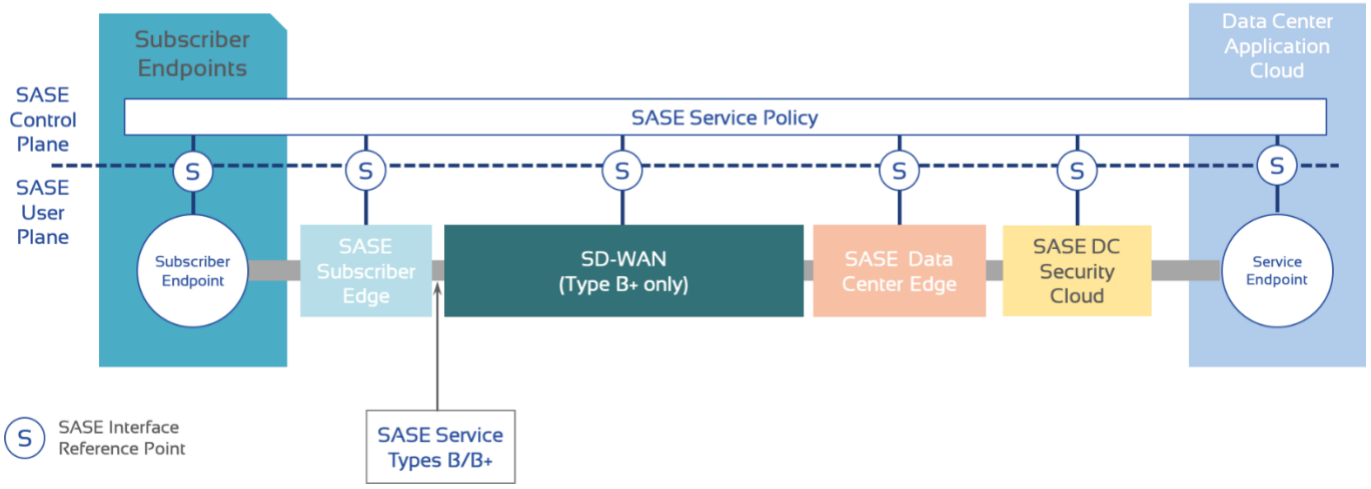

Figure 8: SASE Service Types B/B+

SASE considerations for DC Application Cloud: The DC Application Cloud is one that is controlled by the customer, regardless of whether it be on-premise or in a Co-Lo facility. This maps to the Endpoint and Edge framework elements.

SASE Service Component	Subscriber Endpoint	Subscriber Edge	SD-WAN (Service Type B+ only)	Data Center Edge	Data Center Security Cloud	Service Endpoint in Data Center
Example Implementation	Laptop; Desktop; IP Phone; SmartPhone; App; Server	SD-WAN Edge	MEF 70 SD-WAN managed service	Data Center	Data Center	Payroll; CRM; ERP; ITSM
Example Security Functions	Host FW; HIDS/HIPS	Firewall at SD-WAN Edge Encryption using IPSec and TLS	TVC encryption (optional)	None	FW; UTM; WAF; IPS	NIPS; NIDS; HIPS; HIDS; UTM; FW; WAF
Example Networking Functions	LAN; WiFi	Routing and forwarding	UCS; TVC; SDWC	Routing and Forwarding	None	N/A

Table 4 - Service Type B+ Example

4.1.3 Service Type C/C+

Description: Access to Wholesale Provider Application Cloud

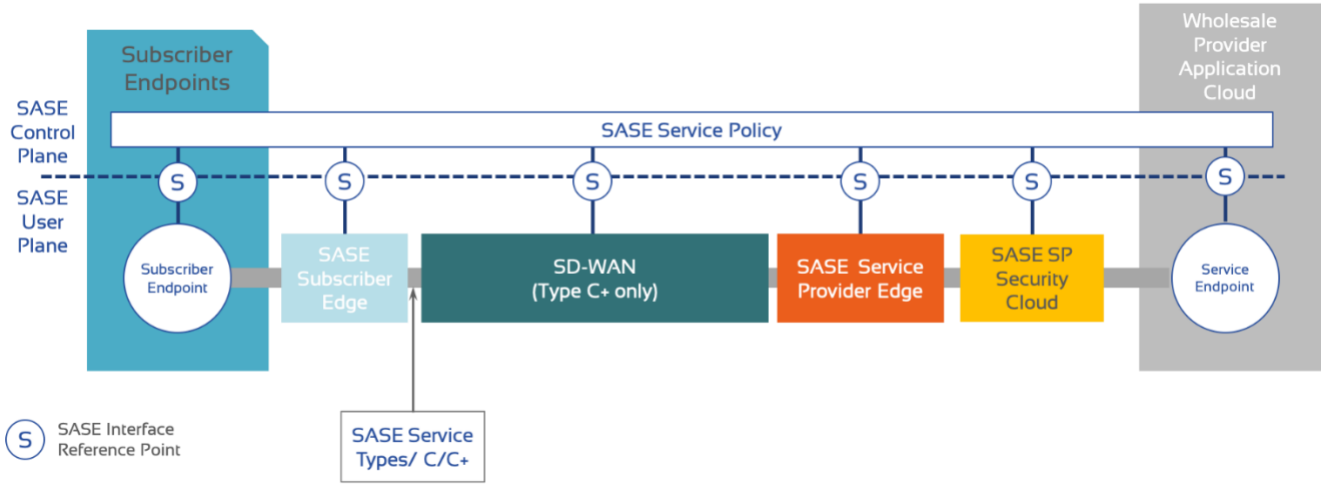

Figure 9: SASE Service Types C/C+

SASE Service Component	Subscriber Endpoint	Subscriber Edge	SD-WAN (Service Type C+ only)	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Wholesale Provider
Example Implementation	Employee on workstation on LAN; Employee on laptop via WiFi	SD-WAN Edge	MEF 70 SD-WAN managed service	Service Provider PoP	Service Provider PoP	SalesForce; Oracle; SAP
Example Security Functions	Embedded endpoint security	Firewall at SD-WAN Edge Encryption using IPSec and TLS	TVC encryption (optional)	No security functions	MBF; DPI; SSL Inspection; DLP; Threat Prevention	Application-level security based on identity and authorization.
Example Networking Functions		Routing and forwarding	UCS; TVC; SDWC	Routing and forwarding including segmentation	No networking functions	No embedded networking functions

Table 5 - Service Type C+ Example

SASE Service Component	Subscriber Endpoint	Subscriber Edge	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Wholesale Provider
Example Implementation	Laptop user working from home	Home WiFi router	Service Provider Cloud	Service Provider Cloud	SalesForce; Oracle; SAP
Example Security Functions	Basic TLS access	None	None	Single sign-on; IAM; CASB; FWaas; ZTNA/SDP; SWG; DLP; Threat protection; Sandbox; BI; CASB.	
Example Networking Functions	DNS or other standard mechanism to steer traffic to SASE service edge.	None	Routing; Proxy; Load balancing; Service chaining; TCP optimization; Caching; CDN	None	

Table 6 - Service Type C Example

4.1.4 Service Type D/D+

Description: Access to Public Internet

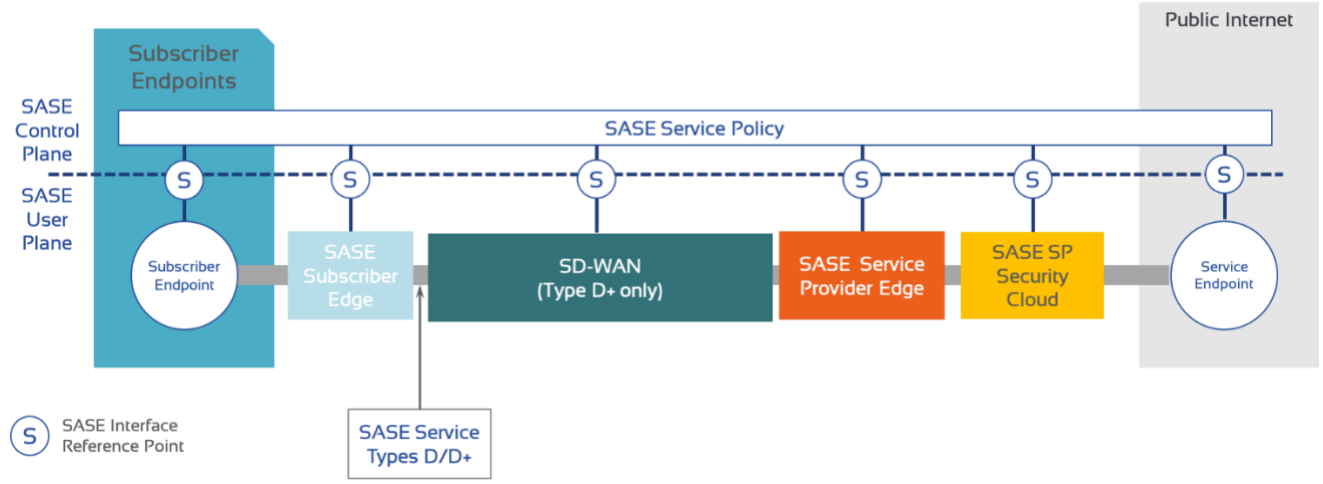

Figure 10: SASE Service Types D/D+

SASE Considerations for the Public Internet: The Public Internet allows any type of traffic to flow through encrypted or unencrypted. There is no SASE-like capability or security in the public space and so, other elements in this model must have security built-in.

SASE Service Component	Subscriber Endpoint	Subscriber Edge	SD-WAN (Service Type D+ only)	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Public Internet
Example Implementation	Laptop; Desktop; SmartPhone	SD-WAN Edge	MEF 70 SD-WAN managed service	Service Provider PoP	Service Provider PoP	Public website
Example Security Functions	Host FW, HIDS/HIPS	Firewall with UTM, IPS and IAM	TVC encryption	N/A, Transit only	Mid-Mile FW; UTM; WAF; IPS	SSL
Example Networking Functions	LAN; WiFi	Routing and forwarding	UCS; TVC; SDWC	IP Transit	IPSec Transit; BGP; Cloud interconnect	None

Table 7 - Service Type D+ Example

SASE Service Component	Subscriber Endpoint	Subscriber Edge	Service Provider Edge	Service Provider Security Cloud	Service Endpoint in Public Internet
Example Implementation	Smartphone; Tablet	None	Service Provider Cloud	Service Provider Cloud	Public websites
Example Security Functions	VPN application	None	None	VPN	SSL
Example Networking Functions	4G/5G	None	Routing and forwarding	None	N/A

Table 8 - Service Type D Example

5 Summary

The SASE concept introduced by Gartner is an important first step in understanding how security and software-defined networking can, and should, be integrated in a holistic fashion to support the next generation of digital services. In this White Paper, we have proposed two aspects of a new standardized approach to SASE services. By using the proposed Service Framework approach outlined here, the industry can frame the implementations of each SASE vendor in a comparable way allowing enterprises and service providers the ability to understand the advantages of each vendor approach as well as enabling interoperability between different vendors. Similarly, service providers will be able to use the abstract constructs of SASE services proposed in this document to focus their interactions with enterprise customers that show interest in outsourcing to service providers their security needs around SD-WAN and access to cloud services.

The White Paper will also serve as a starting point for proposed upcoming standardization work around SASE services in MEF.

6 About MEF

An industry association of 200+ member companies, MEF has introduced the MEF 3.0 transformational global services framework for defining, delivering, and certifying assured services orchestrated across a global ecosystem of automated networks. MEF 3.0 services are designed to provide an on-demand, cloud-centric experience with user- and application-directed control over network resources and service capabilities. MEF 3.0 services are delivered over automated, virtualized, and interconnected networks powered by LSO, SDN, and NFV. MEF produces service specifications, LSO frameworks, open LSO APIs, software-driven reference implementations, and certification programs. MEF 3.0 work will enable automated delivery of standardized Carrier Ethernet, Optical Transport, IP, SD-WAN, Security-as-a-Service, and other Layer 4-7 services across multiple provider networks. For more information, visit https://www.mef.net and follow us on LinkedIn and Twitter @MEF_Forum.

7 Terminology

Term	Definition	Reference
BI	Browser Isolation	Wikipedia
CASB	Cloud Access Security Broker	
CDN	Content Delivery Network	
DLP	Data Loss Prevention	
FW	Firewall	
FWaaS	Firewall as a Service	
HIDS	Host-based Intrusion Detection System	
HIPS	Host-based Intrusion Prevention System	
IAM	Identity and Access Management	
IDS	Intrusion Detection System	
IPS	Intrusion Prevention System	
NIDS	Network Intrusion Detection System	

NIPS	Network Intrusion Prevention System
SDP	Software Defined Perimeter
SWG	Secure Web Gateway
UTM	Unified Threat Management
WAF	Web Application Firewall
ZTNA	Zero Trust Network Access

8 References

[1] MEF 70, *SD-WAN Attributes and Services*, August 2019

9 Acknowledgements

- Daniel Bar-Lev (MEF) – Co-Author
- Ron Howell (Datavision) – Co-Author
- Nicolas Thomas (Fortinet) – Contributor
- Marino Wijay (VMware) – Contributor
- Sankar Ramamoorthi (Juniper) – Contributor
- Nico Walters (CMC Networks) – Contributor
- Carl Windsor (Fortinet) – Contributor
- Johan Witters (Nuage) – Contributor
- Neil Danilowicz (Versa Networks) – Contributor
- Charles Eckel (Cisco) – Contributor
- Mark Gibson (Ciena) – Contributor