Spotlight on SASE

19 July 2023, Montréal

MEF

SASE Spotlight Agenda

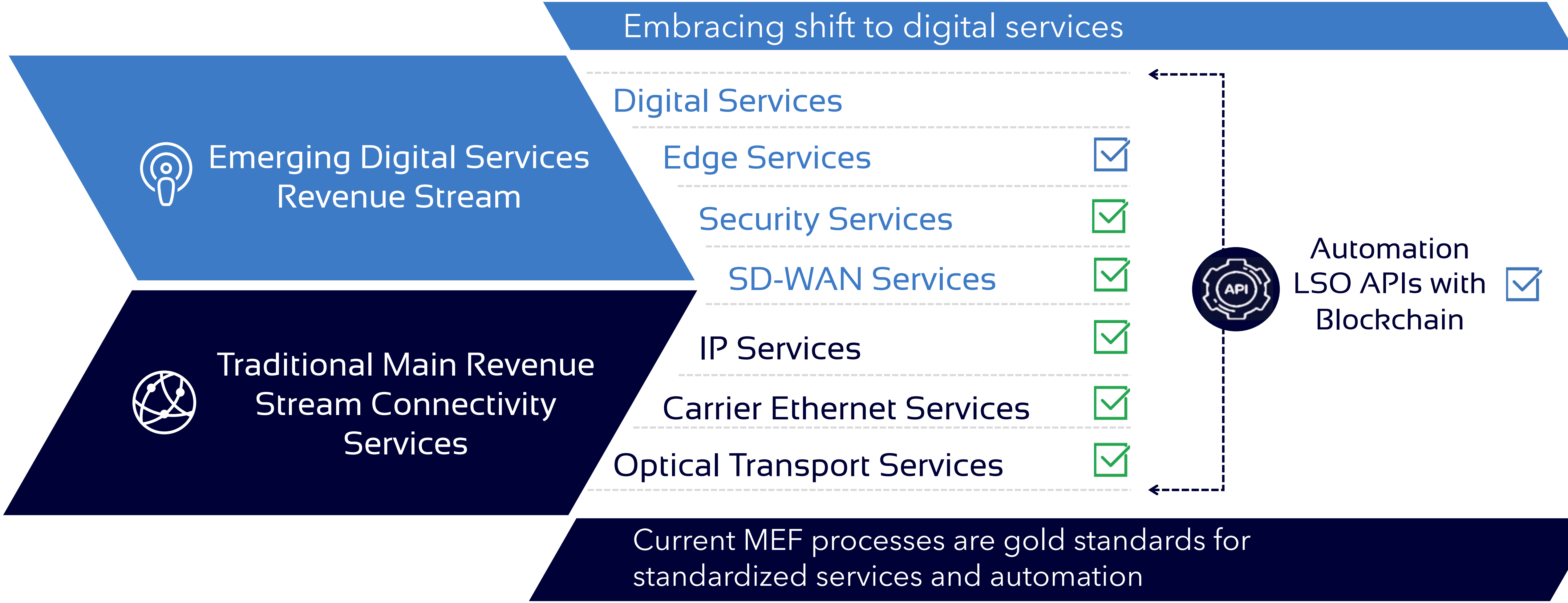
8:30	**Introduction to MEF and SASE**	Pascal Menezes, MEF CTO
8:40	**MEF SASE and SD-WAN Published Work Tutorials**	Larry Samberg, MEF; Neil Danilowicz, Versa
9:30	**MEF SASE & SD-WAN New Standards**	Moderator: Chris Purdy, Head of Prod. Mgmt., Canoga Perkins
10:30	**Break**	
10:40	**SASE Certification / Q&A**	Vikram Phatak, Chairman & CEO, CyberRatings.org
11:20	**SASE Marketing**	Kevin Vachon, COO, MEF
11:25	**SASE Industry Perspectives Panel**	Moderator: Sunil Khandekar, Tech Executive, Advisor, Former Founder and CEO, Nuage Networks
12:15	**Summary and Calls to Action**	Pascal Menezes, CTO, MEF
12:30	**Lunch and Networking**	

Introduction to MEF and SASE

Pascal Menezes
MEF CTO

Spotlight on SASE
19 July 2023

MEF Technical Vision in 2016



Embracing shift to digital services

Emerging Digital Services Revenue Stream

Traditional Main Revenue Stream Connectivity Services

Digital Services

Edge Services 🟦

Security Services 🟩

SD-WAN Services 🟩

IP Services 🟩

Carrier Ethernet Services 🟩

Optical Transport Services 🟩

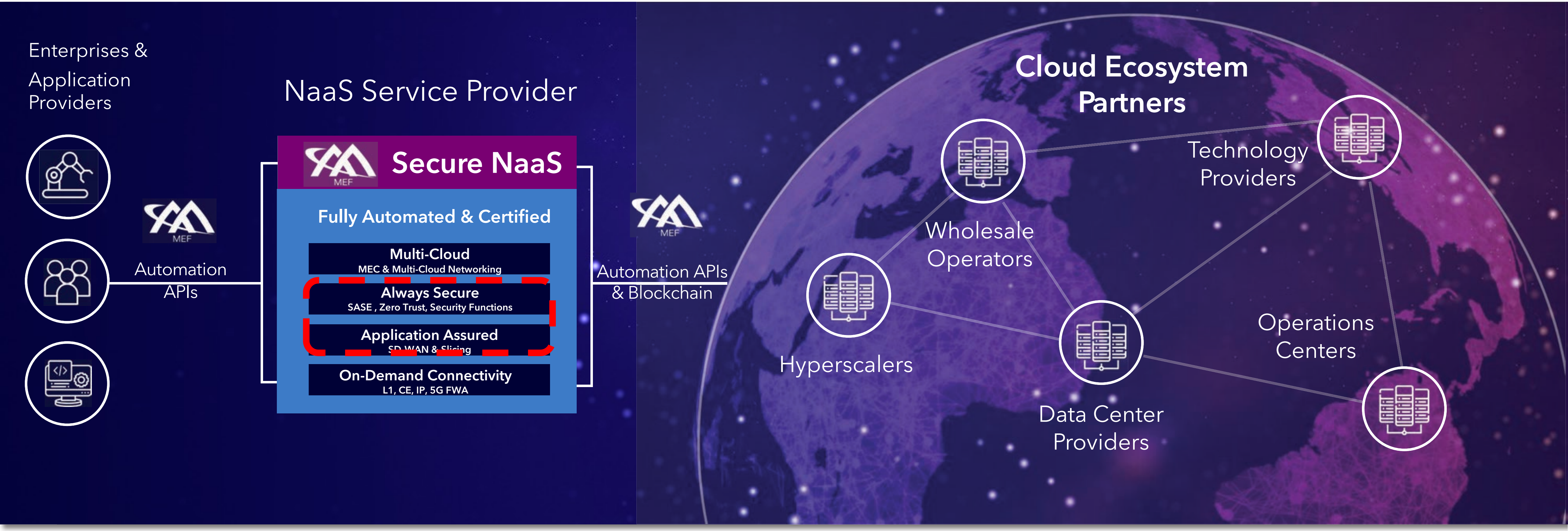
Automation LSO APIs with Blockchain 🟦

Current MEF processes are gold standards for standardized services and automation

🟩 Complete 🟦 Almost Complete 🟧 Just Started

MEF’s NaaS Current Vision

A Blueprint for Services, Certification and Automating the Global Ecosystem



Enterprises & Application Providers

Automation APIs

NaaS Service Provider

Secure NaaS

Fully Automated & Certified

Multi-Cloud
MEC & Multi-Cloud Networking

Always Secure
SASE , Zero Trust, Security Functions

Application Assured
SD WAN & Slicing

On-Demand Connectivity
L1, CE, IP, 5G FWA

Automation APIs & Blockchain

Cloud Ecosystem Partners

Wholesale Operators

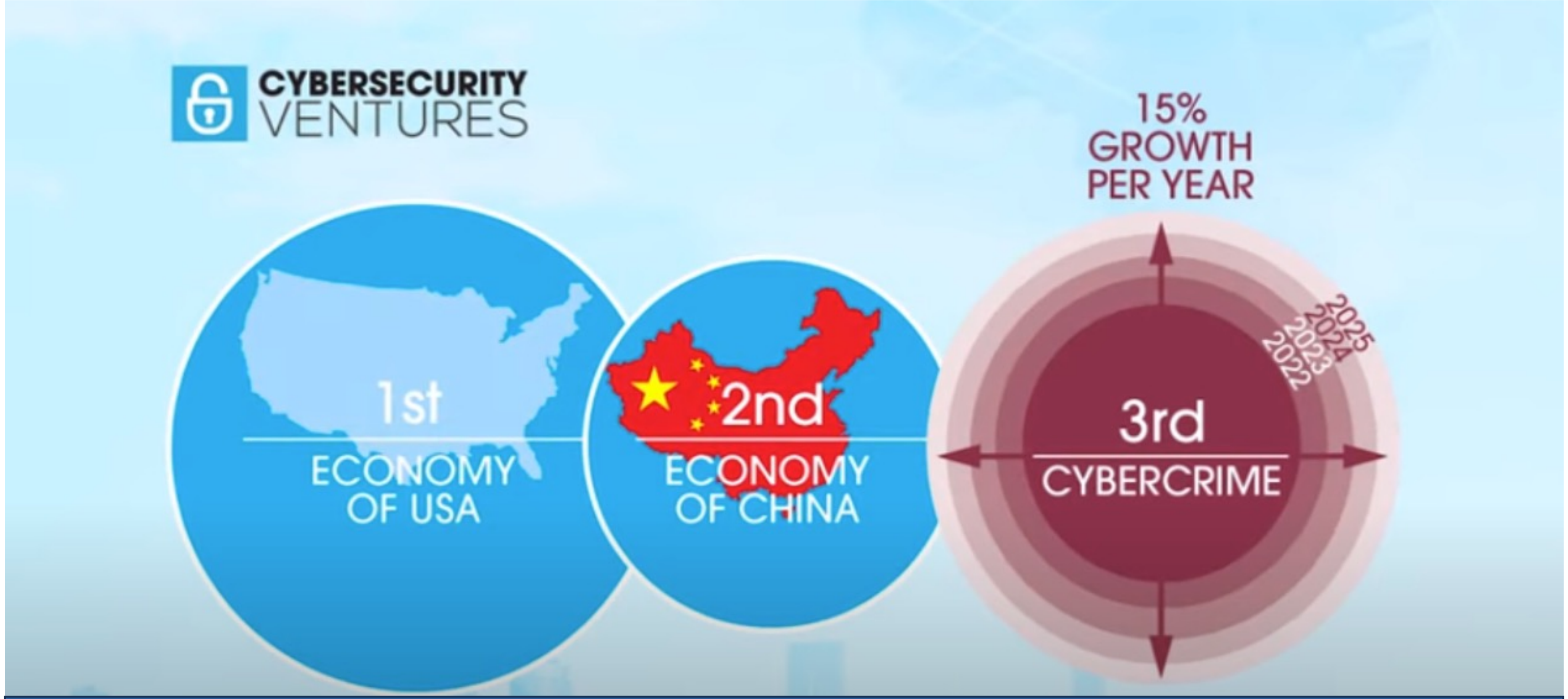
Technology Providers

Hyperscalers

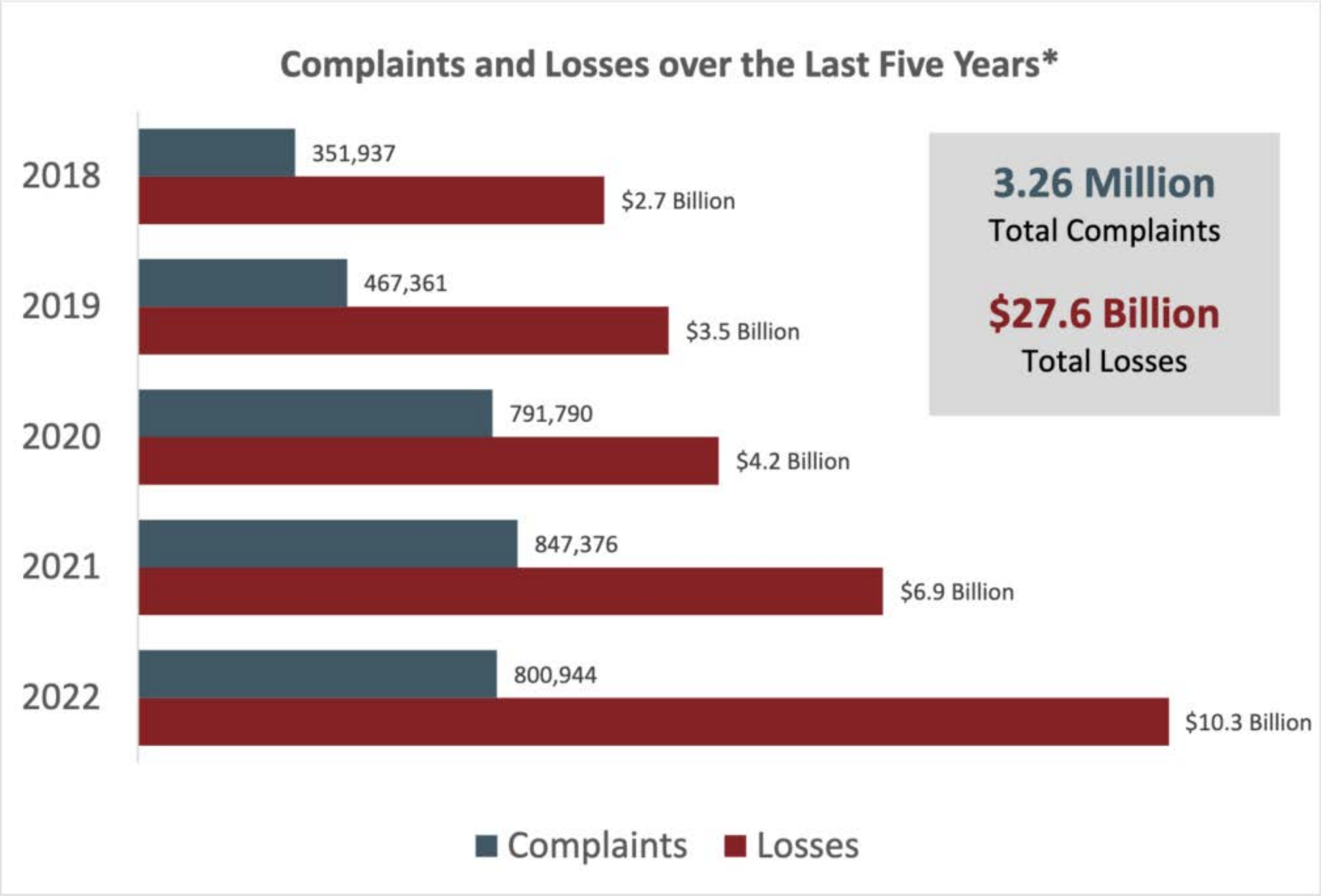
Data Center Providers

Operations Centers

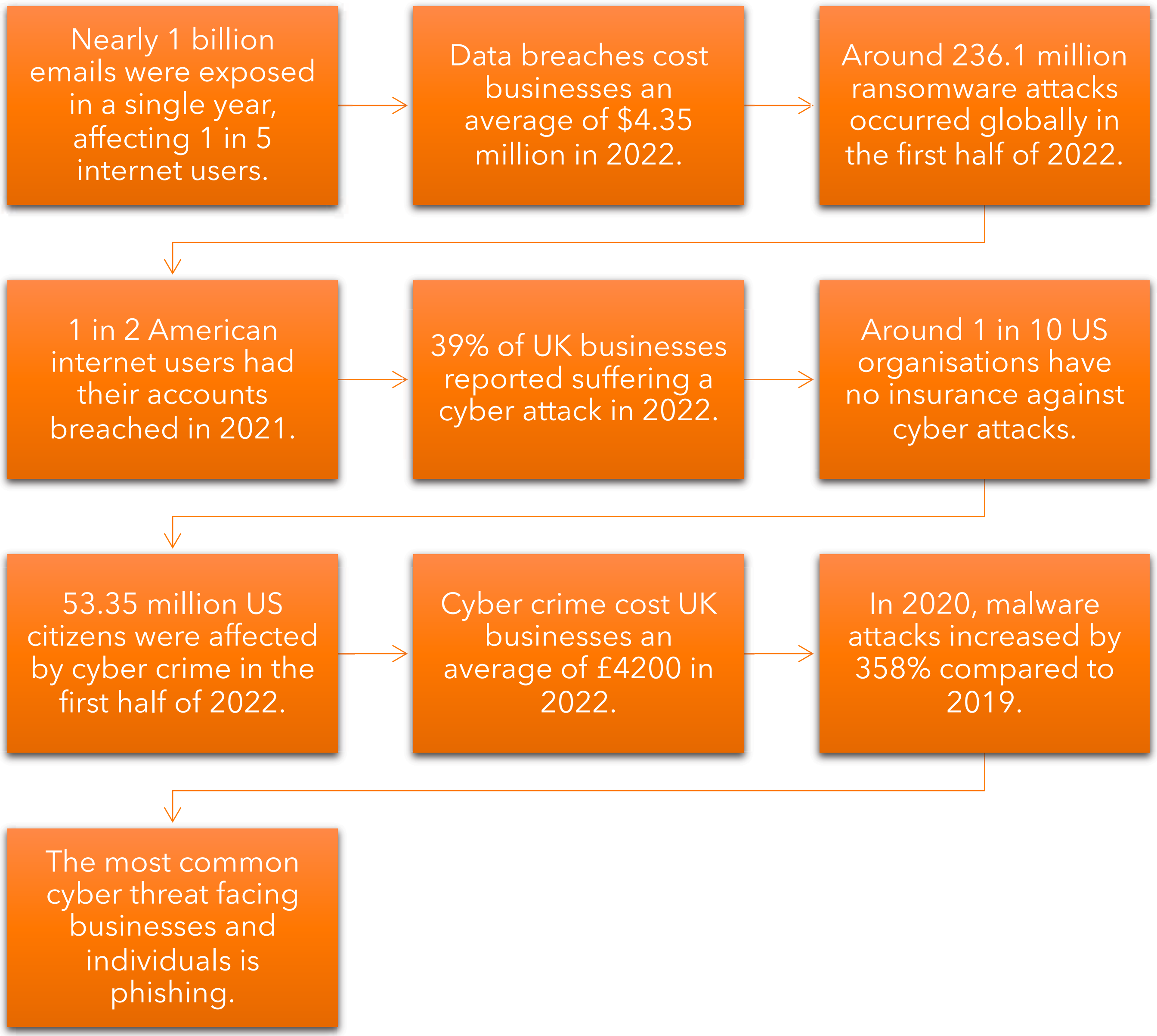
Cybercrime is the Third Largest Economy



Cybercrime Losses Exceeded $10 Billion in 2022: FBI



Cybercrime Statistics



Nearly 1 billion emails were exposed in a single year, affecting 1 in 5 internet users.

Data breaches cost businesses an average of $4.35 million in 2022.

Around 236.1 million ransomware attacks occurred globally in the first half of 2022.

1 in 2 American internet users had their accounts breached in 2021.

39% of UK businesses reported suffering a cyber attack in 2022.

Around 1 in 10 US organisations have no insurance against cyber attacks.

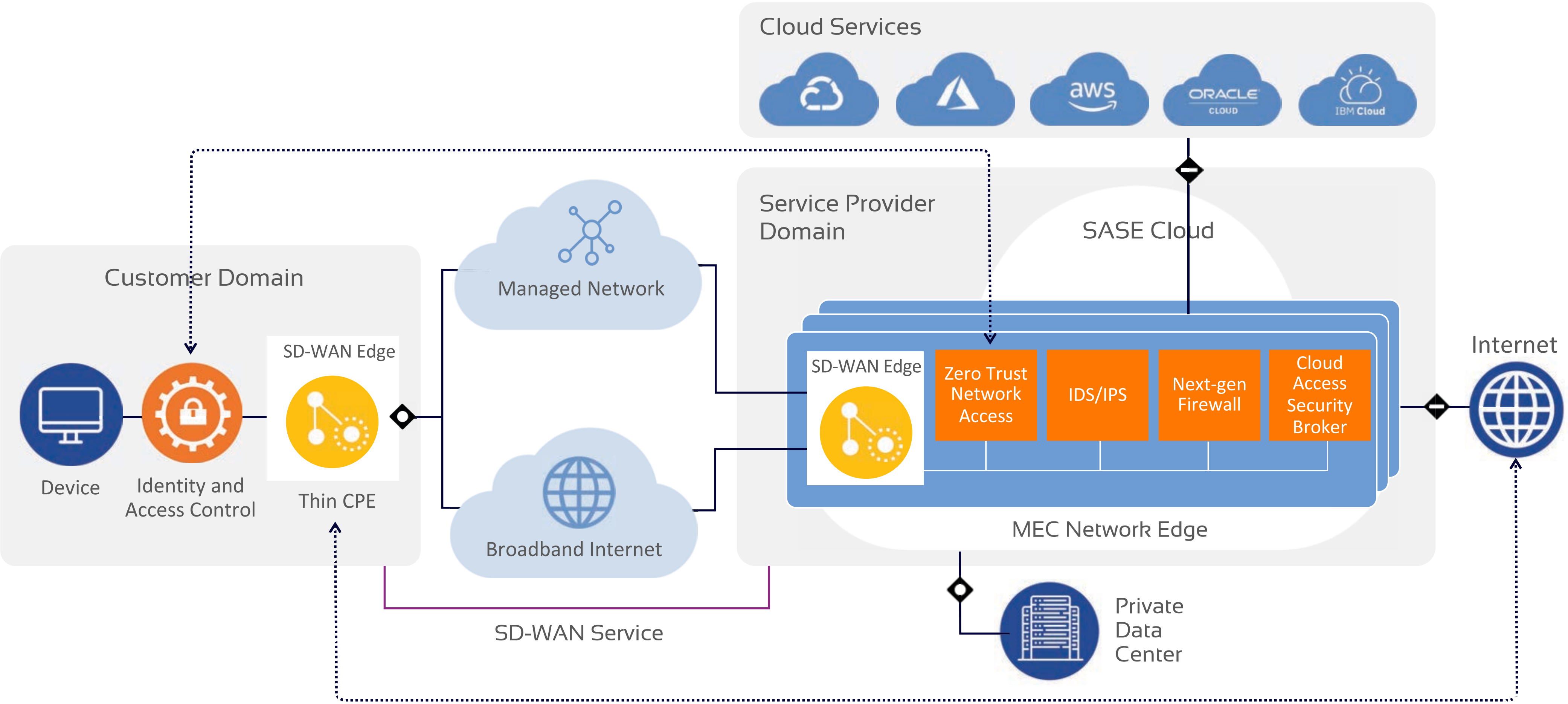
53.35 million US citizens were affected by cyber crime in the first half of 2022.

Cyber crime cost UK businesses an average of £4200 in 2022.

In 2020, malware attacks increased by 358% compared to 2019.

The most common cyber threat facing businesses and individuals is phishing.

Secure Access Service Edge (SASE)



MEF SD-WAN, SASE and Zero Trust Work Activities

Application Assurance

SD-WAN

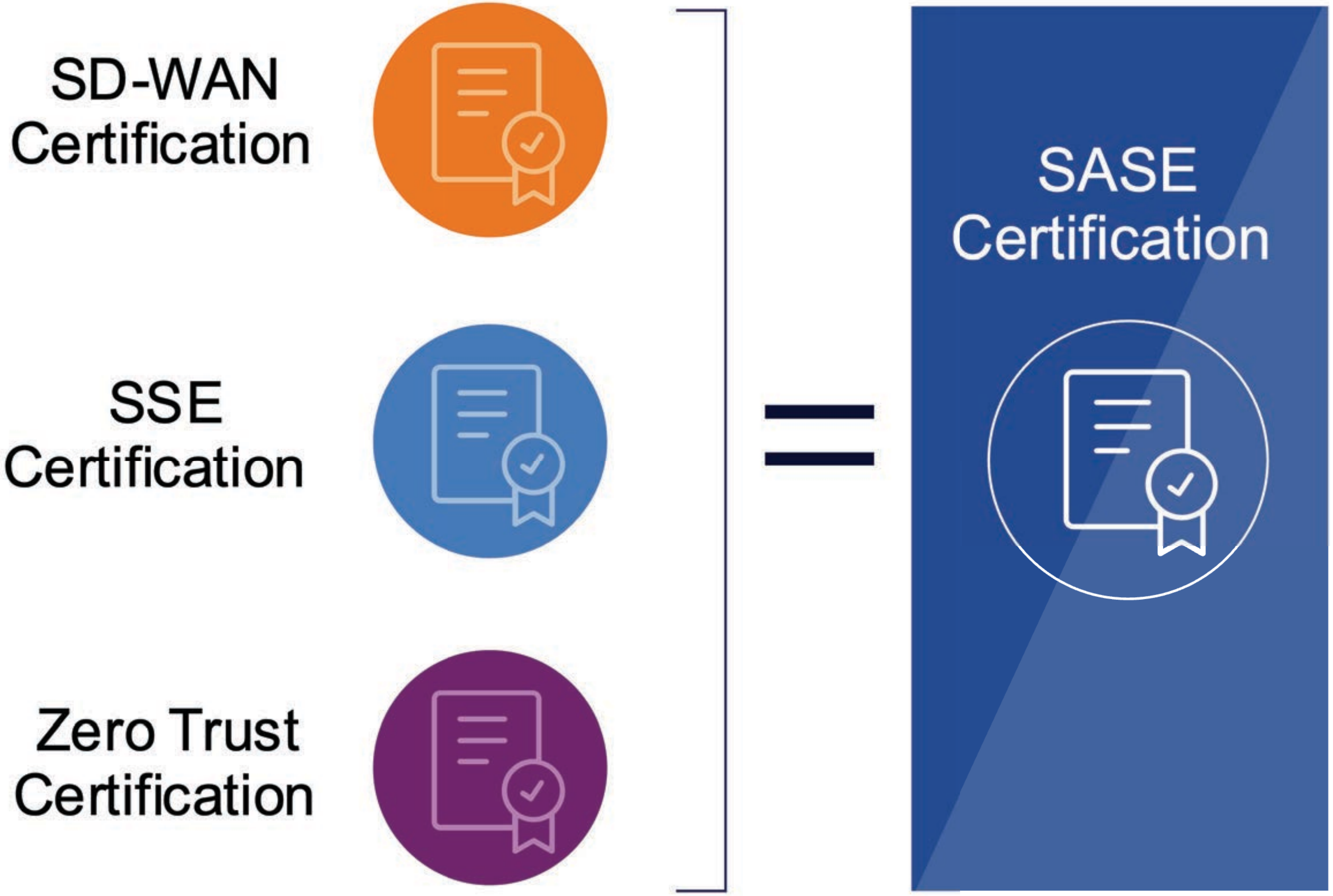
Publish	Active	SD-WAN Standards
MEF 70.1	MEF 70.2	SD-WAN Service Attributes and Service Framework
MEF 105	MEF W105	Draft R5 Performance Monitoring and Service Readiness Testing for SD-WAN
	MEF W119	Universal SD-WAN Edge

Cybersecurity

SASE, Zero Trust and Application Security for IP Services

Publish	Active	Cybersecurity Standards
MEF 117	IG	SASE Service Attributes and Services Framework
MEF 118	IG	Zero Trust Framework for MEF Services
	IG	Secure Service Edge Attributes
	MEF W138	Security Functions for IP-based Services
MEF 88		Application Security for SD-WAN Services

MEF SASE Certification – 3 Certification Options



SD-WAN Certification

SSE Certification

Zero Trust Certification

=

SASE Certification

MEF SASE Certification Value

Enable Enterprise Value With Critical Areas of Testing

- WAN Impairments
- Scale Performance
- Classification Verification
- Threat Protection
- TLS/SSL Functionality
- Zero Trust
- Compliance to MEF Standards

Transition to a CI/CD Cloud Model

- Cybersecurity postures has to be tested at least every 30 days for threat protection
- Major releases must be retested
- Delivers a high degree of SASE service confidence to enterprise

MEF SD-WAN, ZT and SASE Published Work Tutorials

Larry Samberg

MEF, SD-WAN Service Attributes (MEF 70.1)

Chris Purdy

VP Product Management, Canoga Perkins, DSC Co-chair

Neil Danilowicz

Principal Architect, Versa Networks, SASE Service Attributes (MEF 117)

Spotlight on SASE
19 July 2023

MEF 3.0 SD-WAN Services

July 2023

MEF SD-WAN Standard
MEF 70.1 and MEF 70.2

MEF SD-WAN Service Standard (MEF 70.1/MEF 70.2)

MEF’s **SD-WAN Service Attributes and Service Framework (MEF 70.x)** standard is the industry global standard defining SD-WAN services.

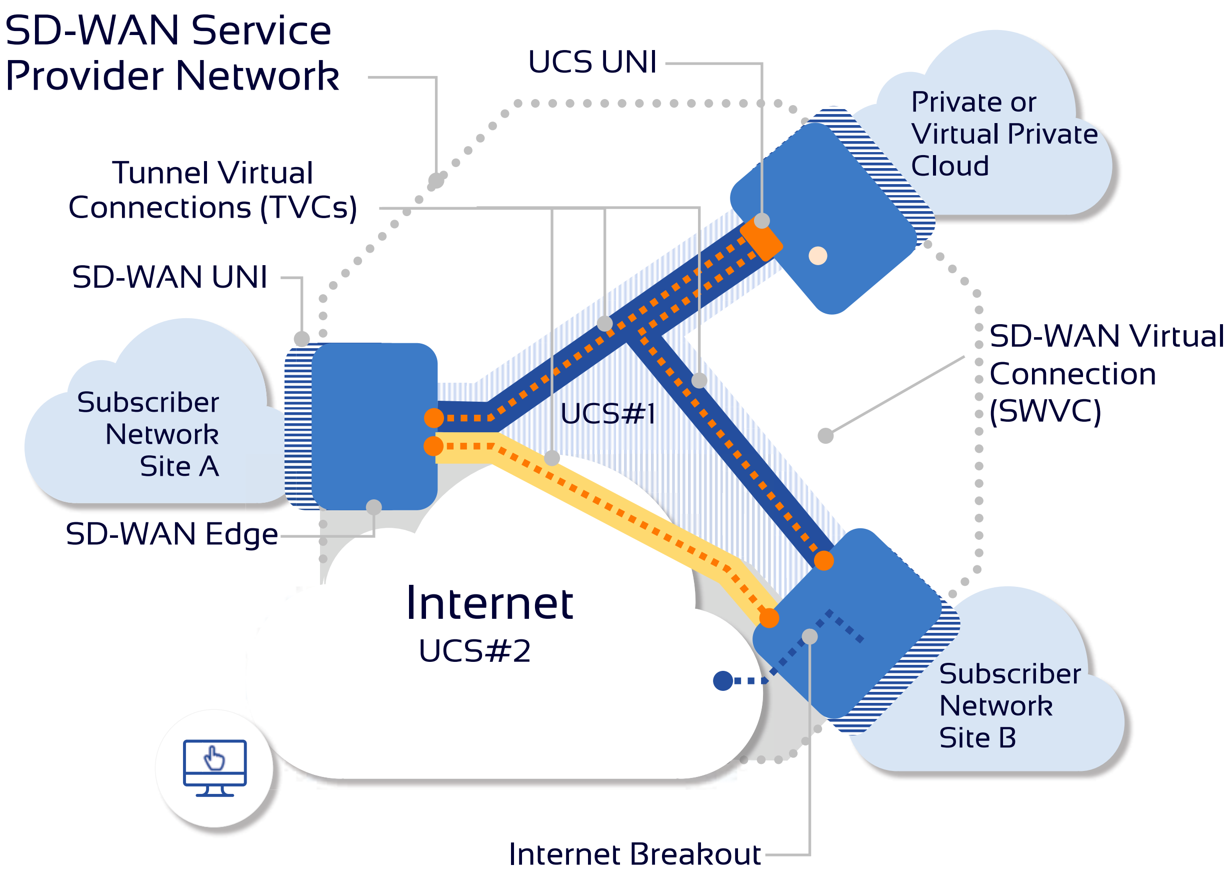
It describes requirements for an application-aware, over-the-top WAN connectivity service that uses policies to determine how application flows are directed over multiple underlay networks irrespective of the underlay technologies or service providers who deliver them.

Service Definition and Service Attributes

- A Service Attribute captures specific information about the behavior of the Service that is agreed on between the **Subscriber** of the service (buyer) and the **Provider** of the service (seller).
- Service Attributes are specified for the Service (SWVC), each Service End Point at a UNI, each UNI. There are also some Service Attributes relating to the Underlay Connectivity Services.
- The "agreement" on a value for a Service Attribute can be reached in several ways, for example:
  - The Service Provider mandates a particular value.
  - The Subscriber selects from a set of options specified by the Service Provider.
  - The Subscriber requests a particular value, and the Service Provider accepts it.
  - The Subscriber and Service Provider negotiate to reach a mutually acceptable value.
  - The value is derived from the value of another Service Attribute

MEF

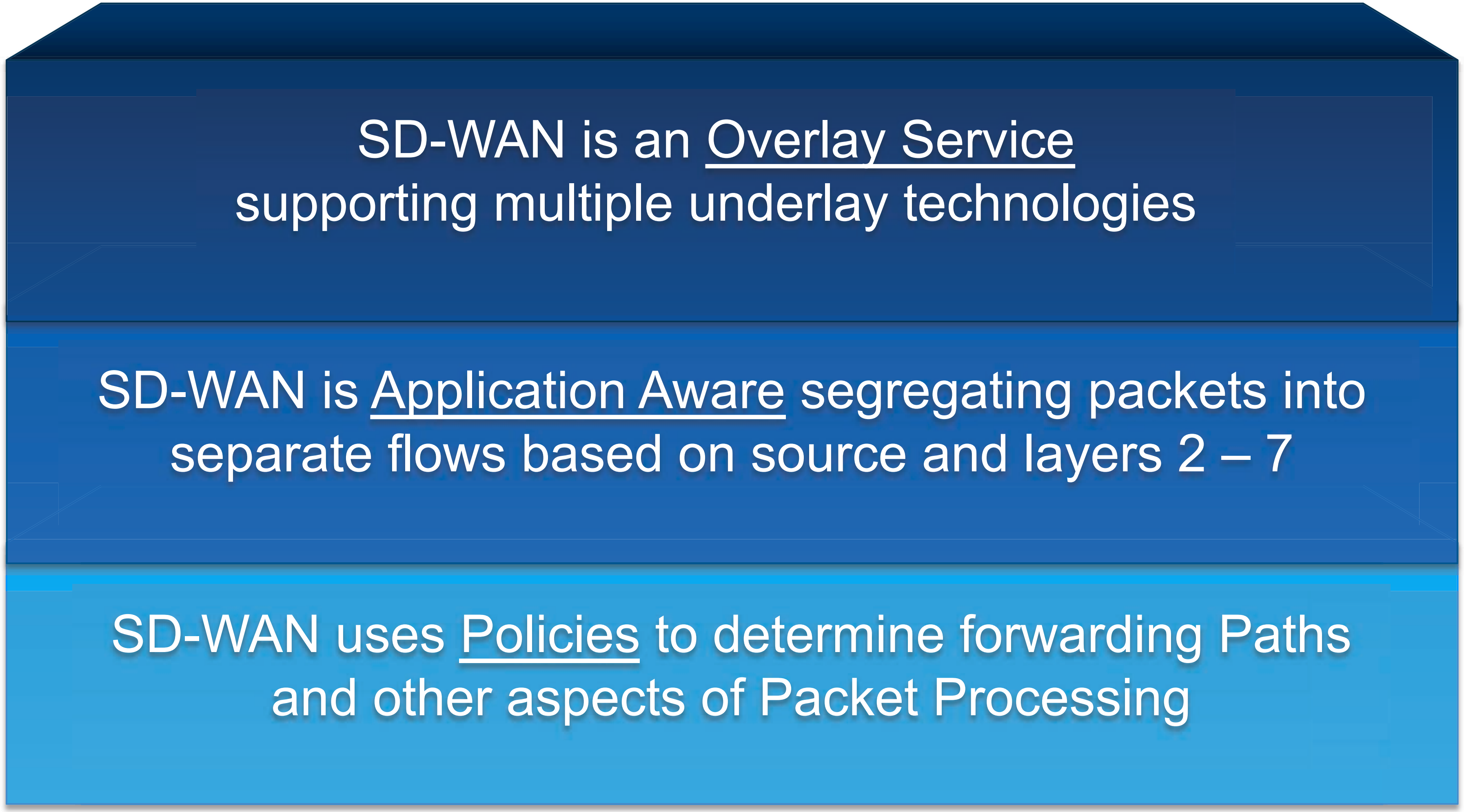
SD-WAN Service Components



SD-WAN Service Provider Network
UCS UNI
Tunnel Virtual Connections (TVCs)
SD-WAN UNI
Private or Virtual Private Cloud
SD-WAN Virtual Connection (SWVC)
Subscriber Network Site A
UCS#1
SD-WAN Edge
Internet
UCS#2
Subscriber Network Site B
Internet Breakout

- **SD-WAN User to Network Interface (UNI)**
  Demarcation between Service Provider and Subscriber responsibility
- **SD-WAN Virtual Connection (SWVC)**
  Logical multipoint connection between the SD-WAN UNIs that corresponds to the SD-WAN Service
- **SD-WAN Virtual Connection End-Point (SWVC EP)**
  Logical point where application flow policies are assigned and applied
- **SD-WAN Edge**
  Connects SD-WAN UNI to UCSs, maps packets to application flows, enforces policies, and selects TVC over which to forward each flow
- **Underlay Connectivity Service (UCS)**
  Any WAN service used by the SD-WAN, e.g., MEF Ethernet Services (MEF 6.2), MEF IP Services (MEF 61.1), MPLS VPNs and Internet Access, and MEF Optical Transport Services (MEF 63)
- **Tunnel Virtual Connection (TVC)**
  Point-to-point paths across UCSs that compose an SD-WAN Service
- **Internet Breakout**
  Application Flows forwarded from an SD-WAN UNI directly to the Internet rather than delivered to another SD-WAN UNI.

SD-WAN Is Different From Other MEF Services



SD-WAN is an Overlay Service
supporting multiple underlay technologies

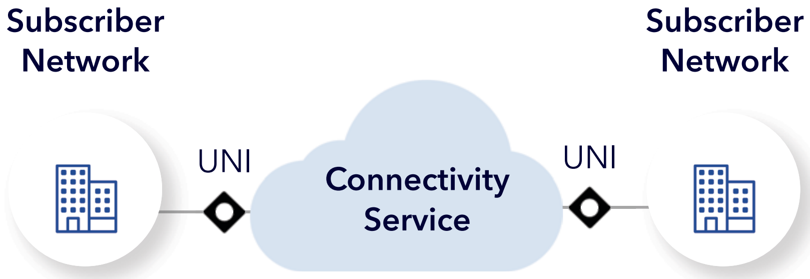
SD-WAN is Application Aware segregating packets into separate flows based on source and layers 2 – 7

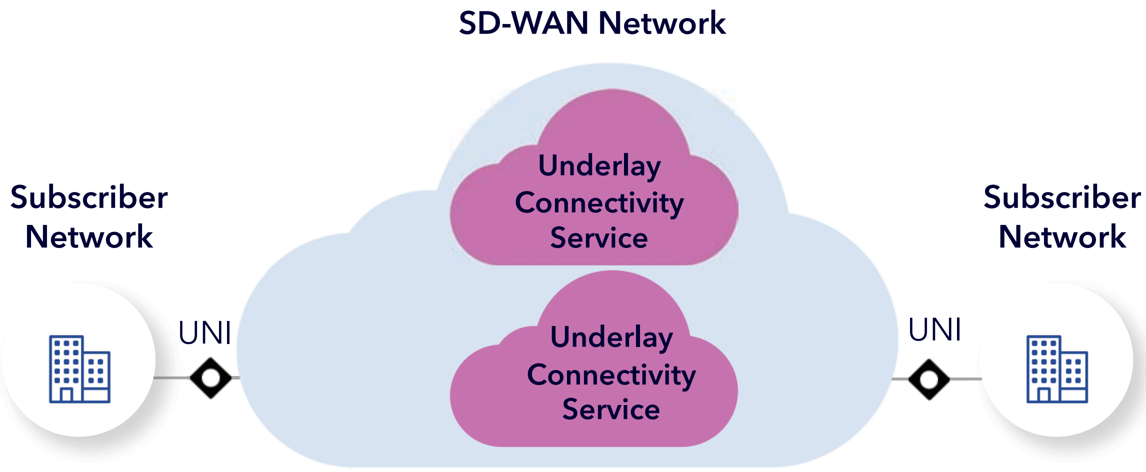
SD-WAN uses Policies to determine forwarding Paths and other aspects of Packet Processing

1. SD-WAN Is An Overlay Service

Connectivity services such as Carrier Ethernet, IP, MPLS, SONET/SDH or OTN are implemented with a single network architecture . The Subscriber connects to the services at UNIs (User-Network Interfaces) and data is transported across that network using the native addressing and forwarding technology of the network architecture – Provider Bridging, IP Routing, Label Switching, etc. (left diagram)

SD-WAN provides an Overlay on multiple connectivity services that can have the same or different architectures and forwards IP Packets over Paths that are most appropriate for each flow. (right diagram)





2. SD-WAN Is Application Aware

- Traditional network services select the path for packets based on addresses in packet headers using a bridging protocol or routing protocol or port addressing.

- SD-WAN identifies *Application Flows* and forwards each Application Flow over the Path the best satisfies the requirements for that flow.

- Application Flows are identified by inspecting fields in each packet. This inspection can include layer 2 and layer 3 (network address) but go all the way to layer 7 (application).

- Service Providers can provide a catalog that can include both simple and complex Application Flow Specifications.

3. SD-WAN Forwarding is Policy-Based

- SD-WAN identifies Application Flows and forwards each Application Flow over the Path the best satisfies the requirements for that flow.

- This is accomplished by applying a Policy to each Application Flow.

- Each Policy contains rules about how to process and forward the Application Flow. For example:
  - Is encryption required for the Application Flow?
  - Can the Application Flow traverse the public Internet? (If the Internet is an Underlay network)
  - Are there bandwidth constraints on the Application Flow?
  - Which performance metrics are important to the Application Flow (loss, delay, etc.)?
  - Which UNIs can the Application Flow be delivered to?
  - Etc.

SD-WAN Policy Construction

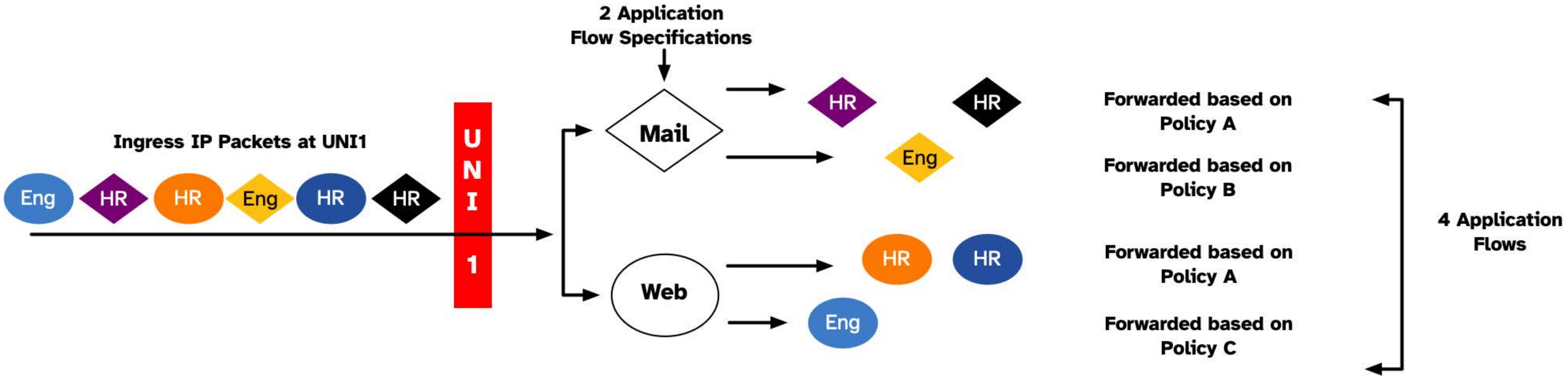
- A **Policy** in MEF 70.1 is a named list of **Policy Criteria**.
- For example:

```
critical, [     ⟨ENCRYPTION, Required-Always⟩,
                ⟨PUBLIC-PRIVATE, Private-only⟩,
                ⟨BILLING-METHOD, Flat-rate-only⟩,
                ⟨BANDWIDTH, 20Mbps, 50Mbps⟩,
                ⟨AF-SECURITY-INGRESS “Paranoid”⟩, (*)
          ]
```

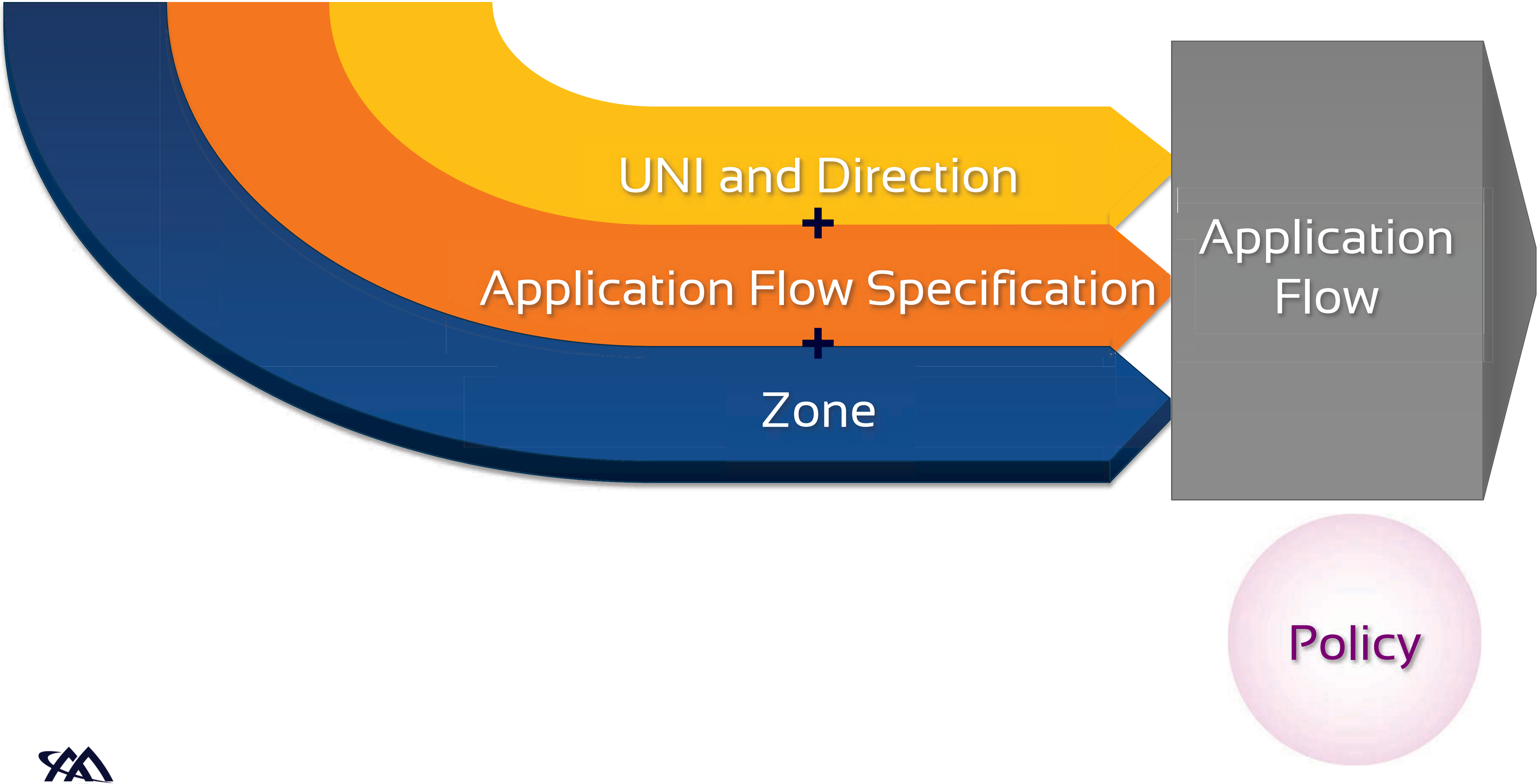
(*) Security Policies are defined in MEF 88, Application Flow Security for SD-WAN Services

Zones

- The Subscriber population can be partitioned into Zones based on IP Address ranges. For example:
  - Zone “Human Resources” is 192.168.1.128/29 and Zone “Engineering” is 192.168.1.192/26
- Policies are assigned to Application Flows


2 Application Flow Specifications
Ingress IP Packets at UNI1
Eng
HR
HR
Eng
HR
HR
UNI 1
Mail
Web
HR
HR
Eng
HR
HR
Eng
Forwarded based on Policy A
Forwarded based on Policy B
Forwarded based on Policy A
Forwarded based on Policy C
4 Application Flows

Application Flow


UNI and Direction

+

Application Flow Specification

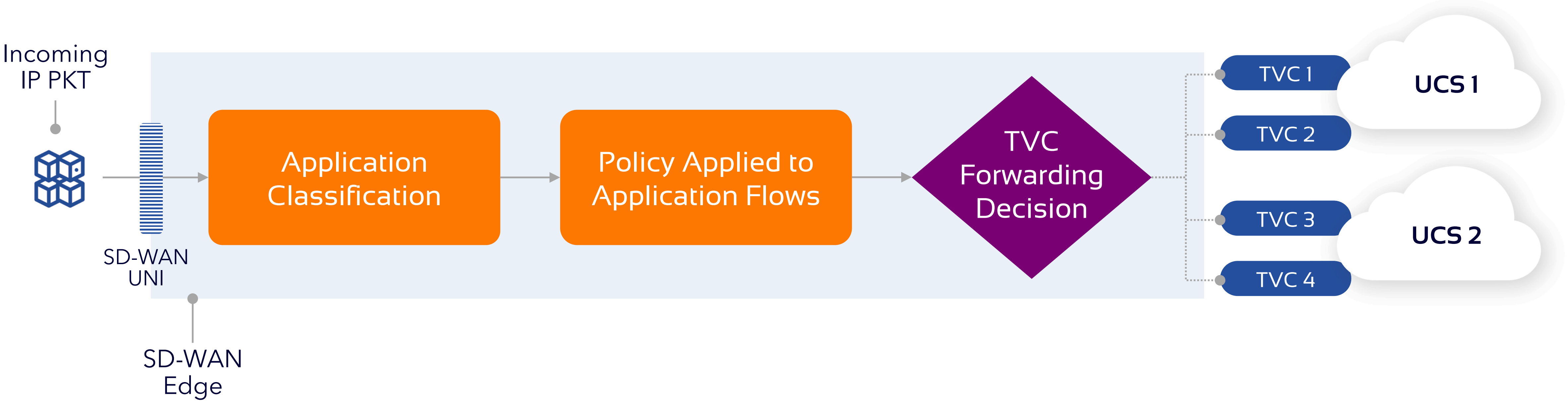
+

Zone

Application Flow

Policy

SD-WAN Application Flow & Policy Function



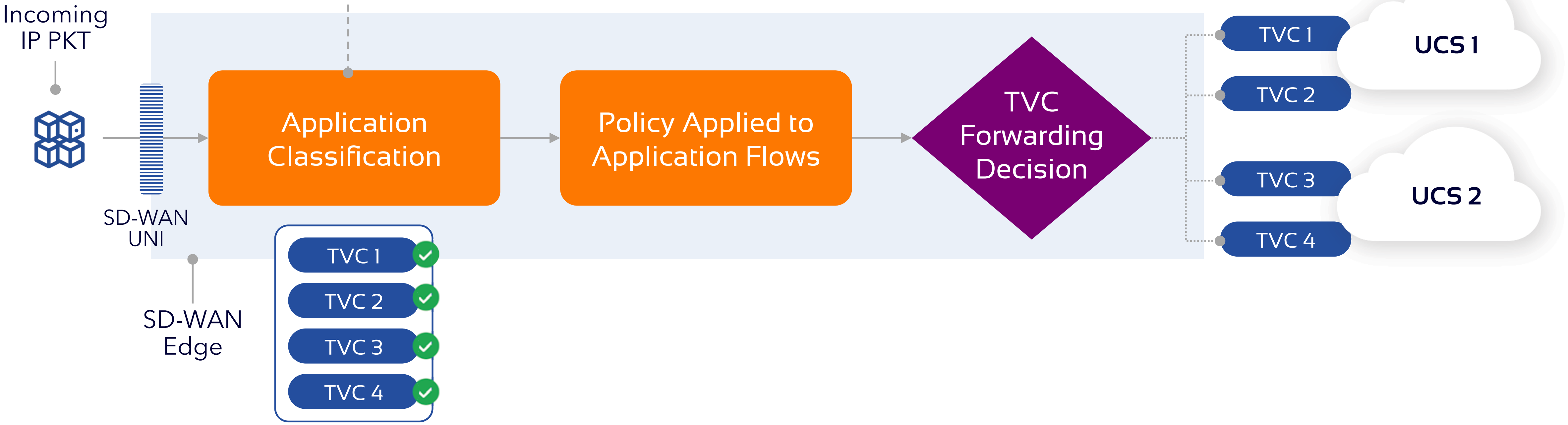
MEF

SD-WAN Application Flow & Policy Function

Example Classification Criteria:

- Src/Dst IP Address
- L4 Protocol
- Src/Dst Port
- Custom match

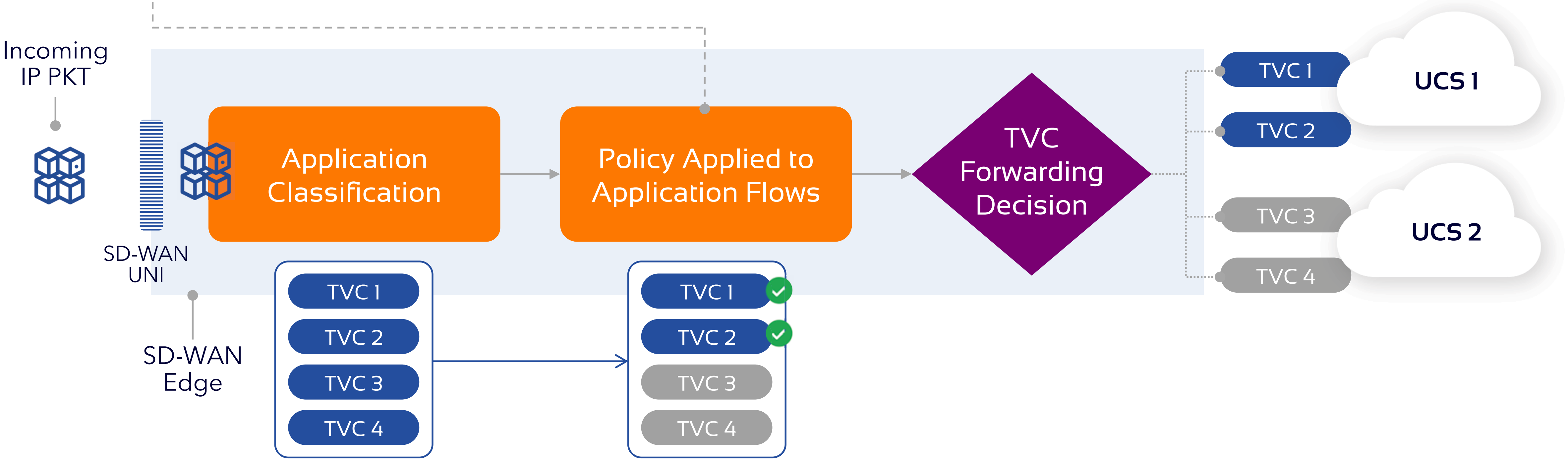
If no Application Flow Specification matches, Packet is discarded



SD-WAN Application Flow & Policy Function

Ingress Policy assigned to the Application Flow

If no Policy is assigned to the Application Flow, all Packets in the Application Flow are discarded



Incoming IP PKT

SD-WAN UNI

SD-WAN Edge

Application Classification

Policy Applied to Application Flows

TVC Forwarding Decision

TVC 1

TVC 2

TVC 3

TVC 4

TVC 1 ✓

TVC 2 ✓

TVC 3

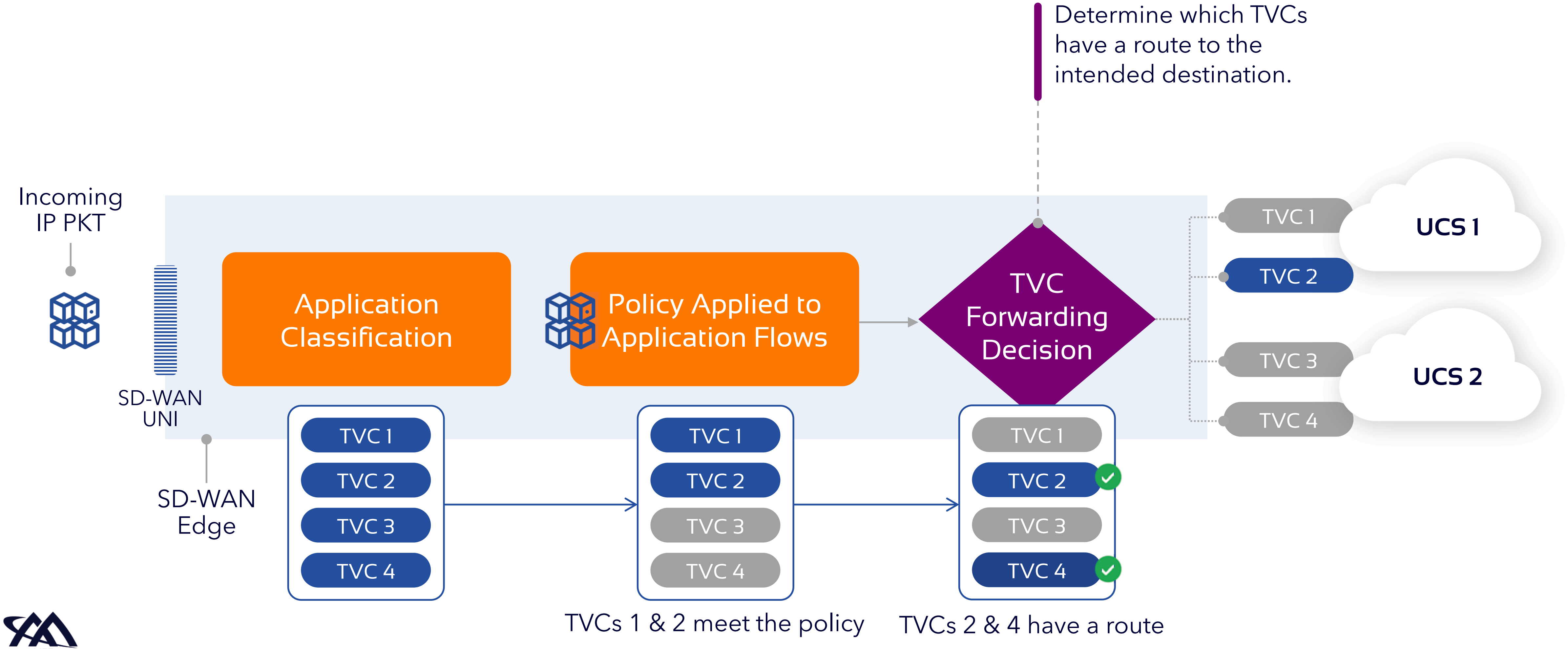
TVC 4

UCS 1: TVC 1, TVC 2

UCS 2: TVC 3, TVC 4

TVCs 1 & 2 meet the policy

SD-WAN Application Flow & Policy Function



Ingress Policies

1. Encryption (Yes, either)
2. Public-private (Private-only, either)
3. Virtual-topology (Virtual Topology Name)
4. Allowed-Egress-Zones (List of Zone Names)
5. Internet-breakout (Yes, No)
6. Billing-method (Flat-Rate-only, Usage-Based-only, Either)
7. Backup (Yes, No)
8. Performance (Subscriber indicates important Metrics for each App. Flow + a bound on acceptable value)
9. Bandwidth (Rate Limiter specification - Committed and Max Rate)
10. AF-Security (*Disabled* or a list of Security functions & associated parameters from MEF 88)
11. Business Importance (Business Importance Label) ★★ New in MEF 70.2

Egress Application Flows and Policies, also

- We normally think about Policies being assigned to Ingress Application Flows.
- But Policies can also be assigned to Egress Application Flows.
- When an IP Packet arrives at an SD-WAN Edge for delivery to a UNI, the IP Packet is categorized to an Egress Application Flow and an Egress Policy can be assigned to it.
- Egress Policies are focused, primarily, on security and are used to decide whether the IP Packet should be forwarded to the Egress UNI or discarded.
- If no Egress Policy is assigned, the Packet is passed to the UNI.
- There are two Egress Policies defined in MEF 70.2:
  - EGRESS BLOCK (allow, discard) (this was called BLOCK-SOURCE before MEF 70.2)
  - AF-SECURITY-EGRESS (Disabled or a list of Security functions & associated parameters from MEF 88)

Improvements and Changes in MEF 70.2

- Business Importance Policy Criterion
  - During periods of resource contention (network failures, traffic overloads, etc.) which Application Flows should be prioritized?
- Improved mechanism for sharing Bandwidth between Application Flows
  - Created concept called "Rate Limiter" which can be named or unnamed
  - The BANDWIDTH Policy Criterion specifies a Rate Limiter
  - All Application Flows that are assigned the same "named" Rate Limiter share the Bandwidth parameters specified.
- Enhanced the PEFORMANCE Policy Criterion
  - Added a *Remediation* parameter to indicated when (and if) performance remediation should be engaged for the Application Flow
  - Added a *Ceiling* parameter to indicate when a path switch must be triggered if possible (reduces path switching
- UNI Availability Objective (% of time that the UNI is Available)
- UNI Mean Time To Repair Objective (how long does it take to reestablish a "down" UNI?

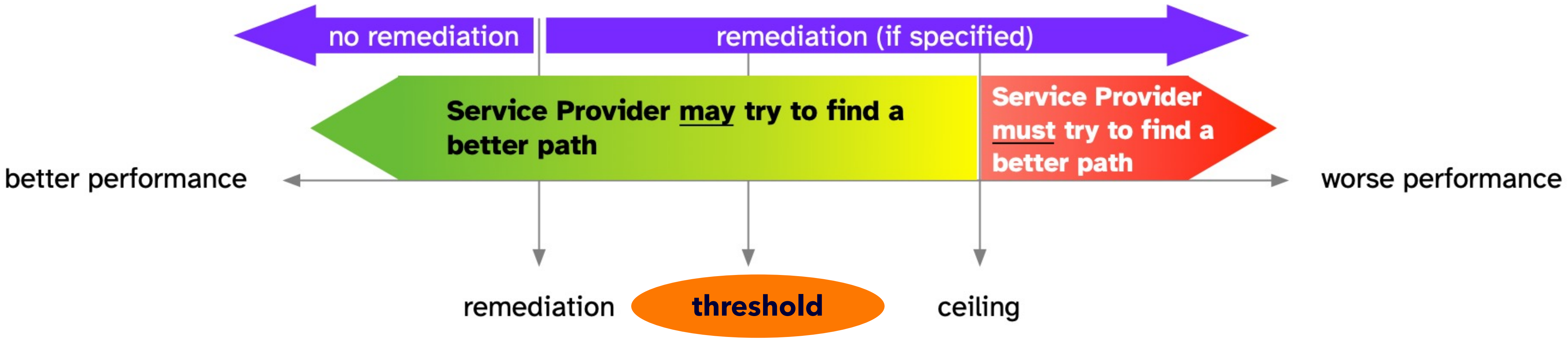
A few minor improvements in MEF 70.2

- For Internet Underlay Connectivity Services is NAT provided by the Service Provider?
- Clarification of information exchanged between the Subscriber and Service Provider about Underlay Connectivity Services provided by the Subscriber.
- Minor Enhancements to INTERNET-BREAKOUT Policy Criterion
- Removed SWVC Service Uptime Service Attribute

Path Selection based on Performance Monitoring

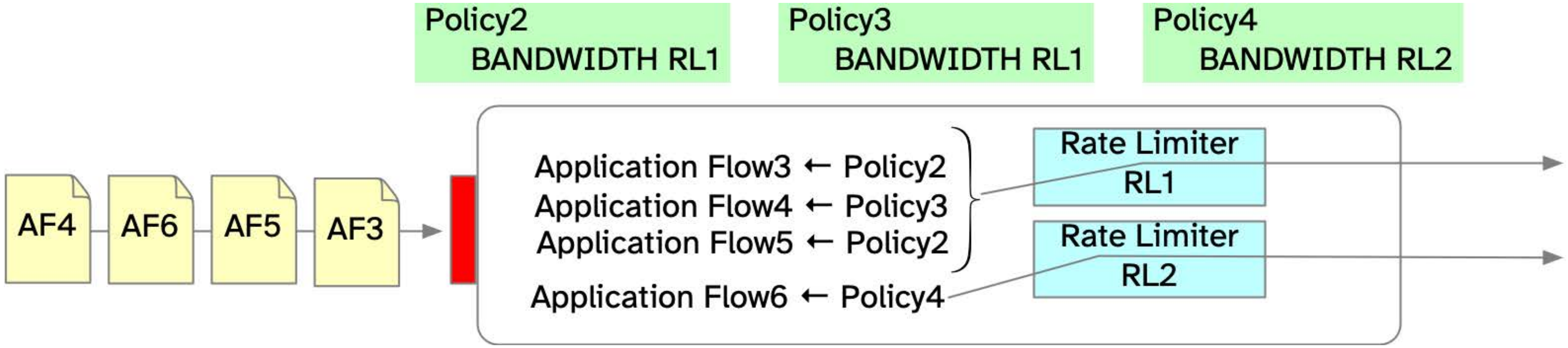
- Policies can specify the important Performance Metric (e.g., delay or loss) and a goal for the Application Flow. For example, the Path delay should be less than 30ms (threshold).

- Paths across the SD-WAN Service can be monitored in real time and the choice of a Path for an Application Flow can be periodically changed to attempt to match the Performance goals specified in the Policy.


no remediation
remediation (if specified)
Service Provider may try to find a better path
Service Provider must try to find a better path
better performance
worse performance
remediation
threshold
ceiling

BANDWIDTH and Rate Limiters

- MEF 70.2 specifies a new concept called a Rate Limiter.
- A Rate Limiter has two parameters: Committed Bandwidth and Maximum Bandwidth (limit).
- A Policy can specify the parameters explicitly:
  - BANDWIDTH ⟨100,300⟩
  - This is an “unnamed” Rate Limiter and is instantiated specifically for the Application Flow to which it is applied (i.e. not shared).
- Alternatively, a list of “named” Rate Limiters can be defined:
  - RL1 = ⟨100,300⟩ RL2 = ⟨100,300⟩ RL3 = ⟨300,400⟩
  - Named Rate Limiters are shared across all of the Application Flows to which they are applied



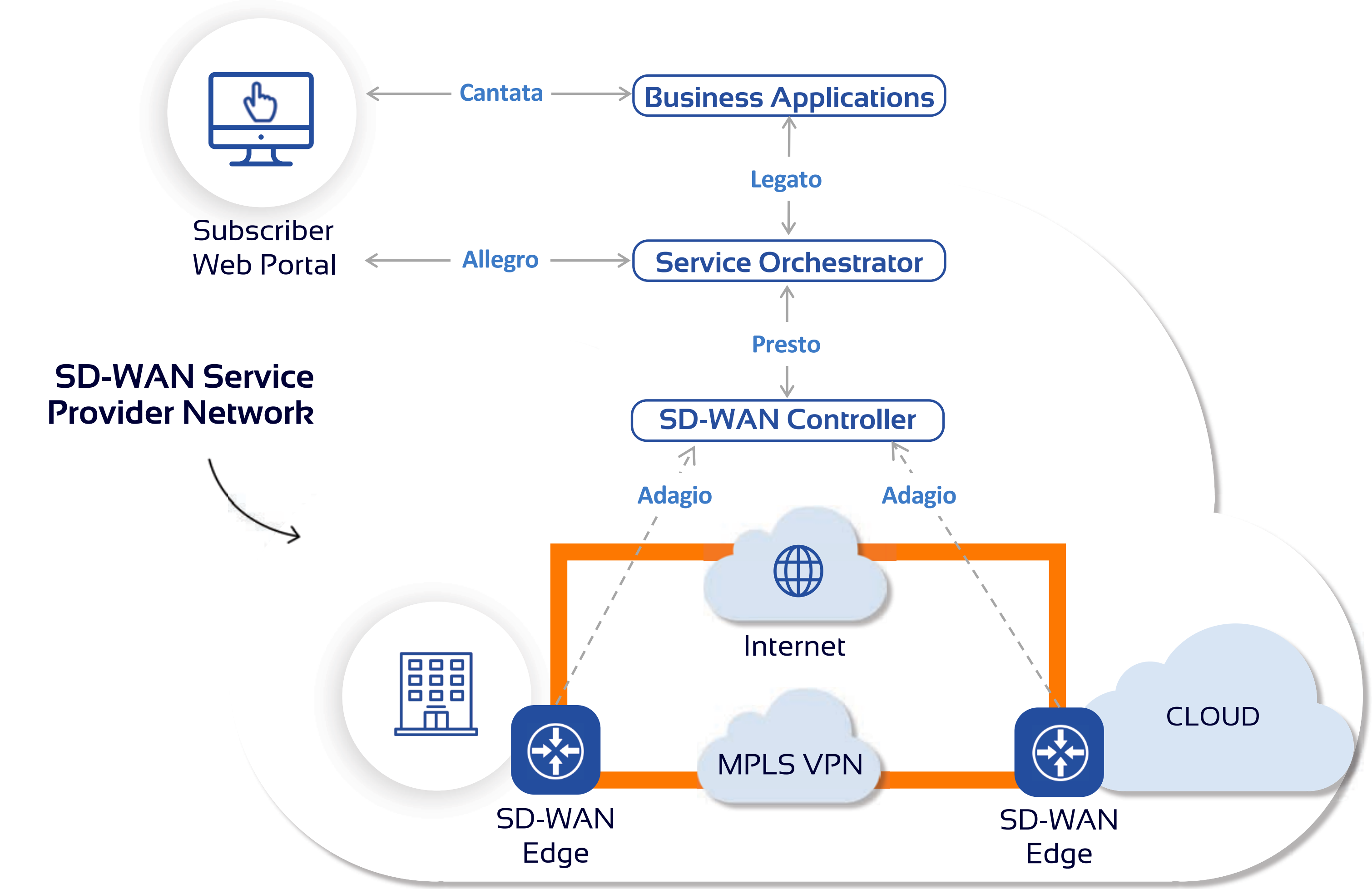
Policy2
BANDWIDTH RL1
Policy3
BANDWIDTH RL1
Policy4
BANDWIDTH RL2
AF4
AF6
AF5
AF3
Application Flow3 ← Policy2
Application Flow4 ← Policy3
Application Flow5 ← Policy2
Application Flow6 ← Policy4
Rate Limiter
RL1
Rate Limiter
RL2

SD-WAN Service Use Cases

USE CASE #1

Hybrid WAN: SD-WAN Service over Internet and MPLS UCSs

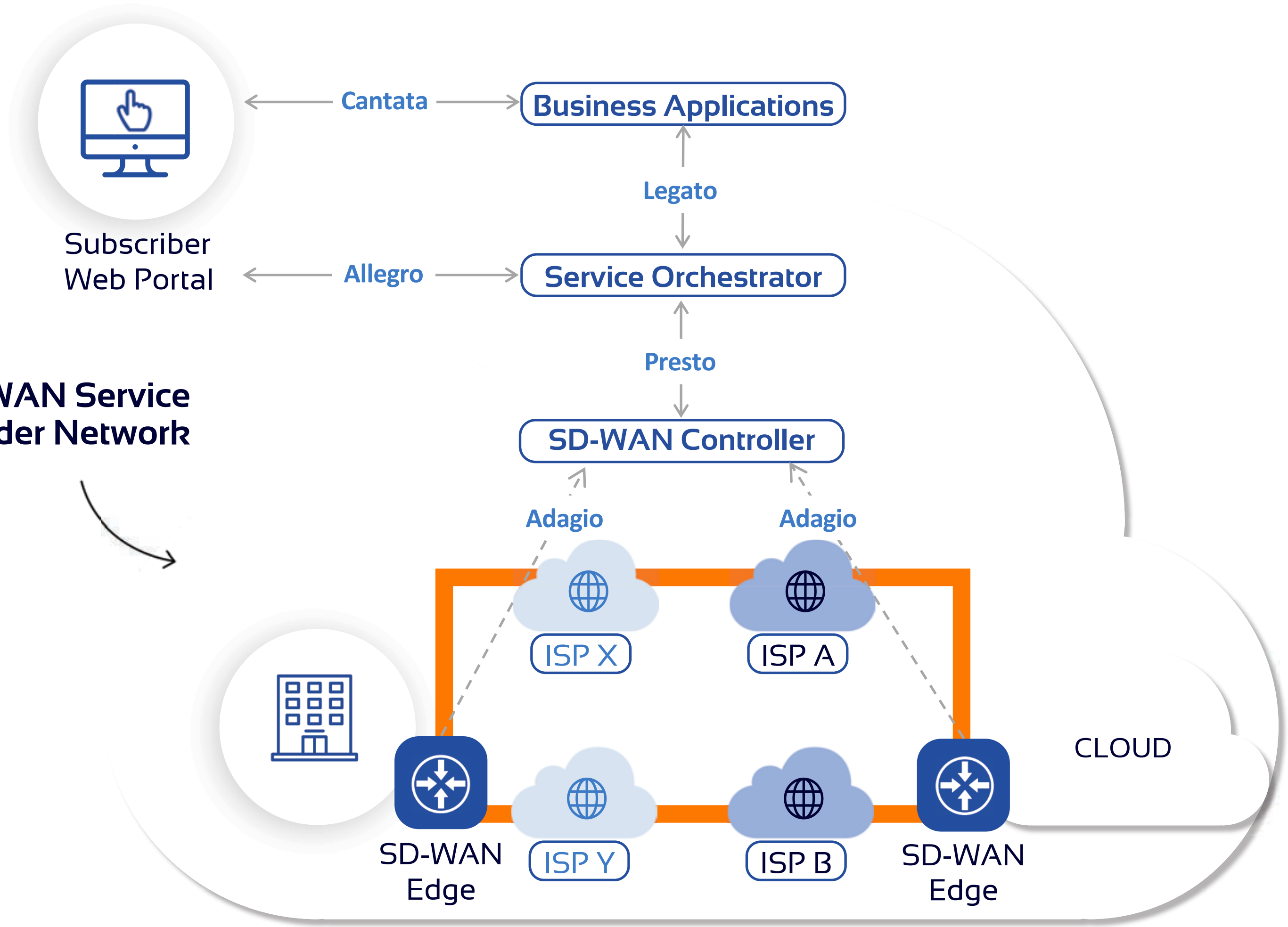
Large Enterprise



- **Encrypted SD-WAN TVCs** over the Internet UCS
- **Allows additional bandwidth** to sites at a lower delivery cost
- **Increased network availability and resiliency**
- **Internet and MPLS VPN UCS** can be provided by different service providers

Dual Internet UCSs: SD-WAN Service over Multiple ISPs

Small Site

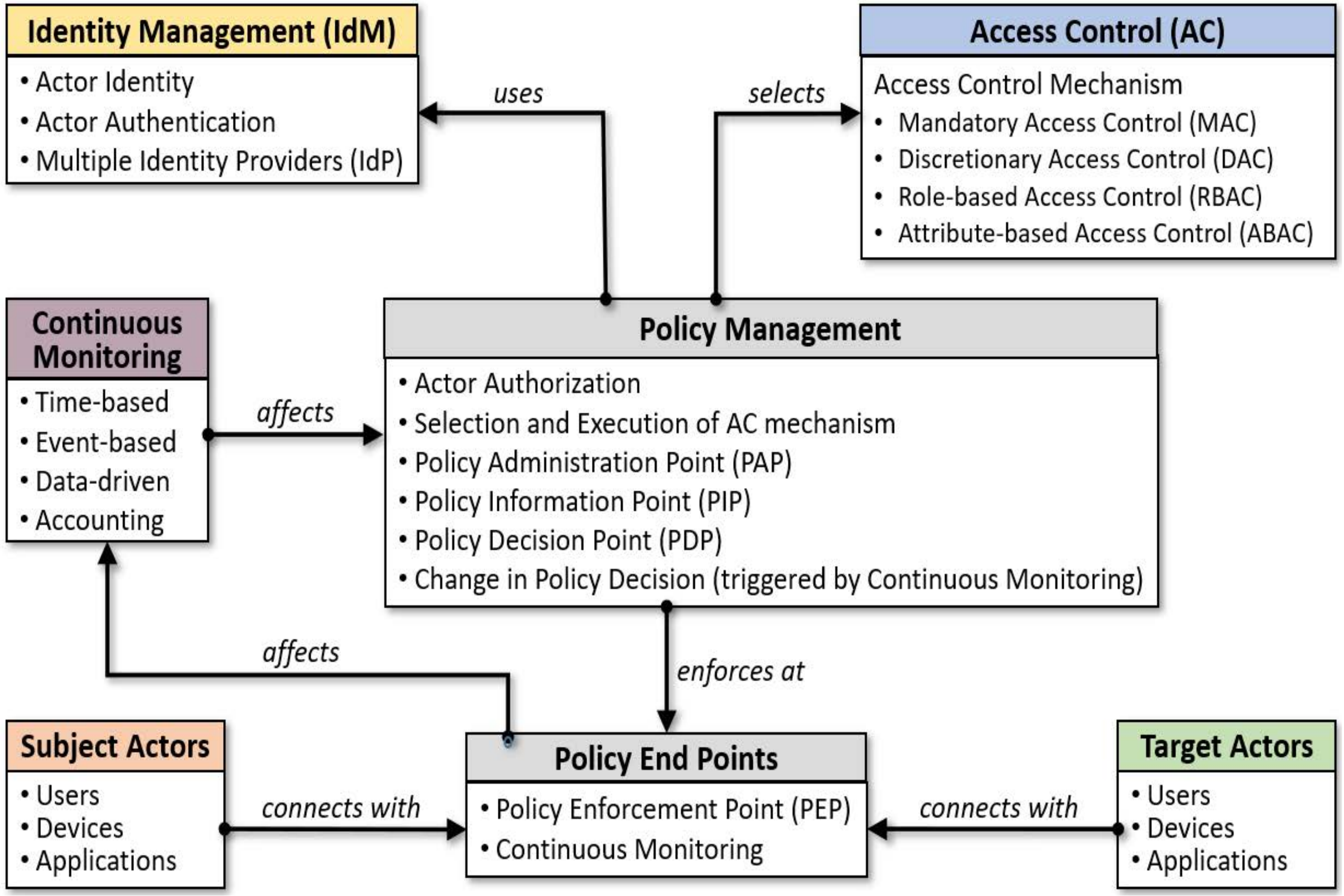


- **Encrypted SD-WAN TVCs** over each Internet UCS from each ISP
- **Using multiple ISPs** achieves provider diversity
- **Increased network availability and resiliency**
- **ISPs may not be the SD-WAN service provider**

MEF 118 Zero Trust Framework for MEF Services

March 2023

Key Elements of MEF's Zero Trust Framework



Identity Management (IdM)
- Actor Identity
- Actor Authentication
- Multiple Identity Providers (IdP)

Access Control (AC)

Access Control Mechanism
- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-based Access Control (RBAC)
- Attribute-based Access Control (ABAC)

Continuous Monitoring
- Time-based
- Event-based
- Data-driven
- Accounting

Policy Management
- Actor Authorization
- Selection and Execution of AC mechanism
- Policy Administration Point (PAP)
- Policy Information Point (PIP)
- Policy Decision Point (PDP)
- Change in Policy Decision (triggered by Continuous Monitoring)

Subject Actors
- Users
- Devices
- Applications

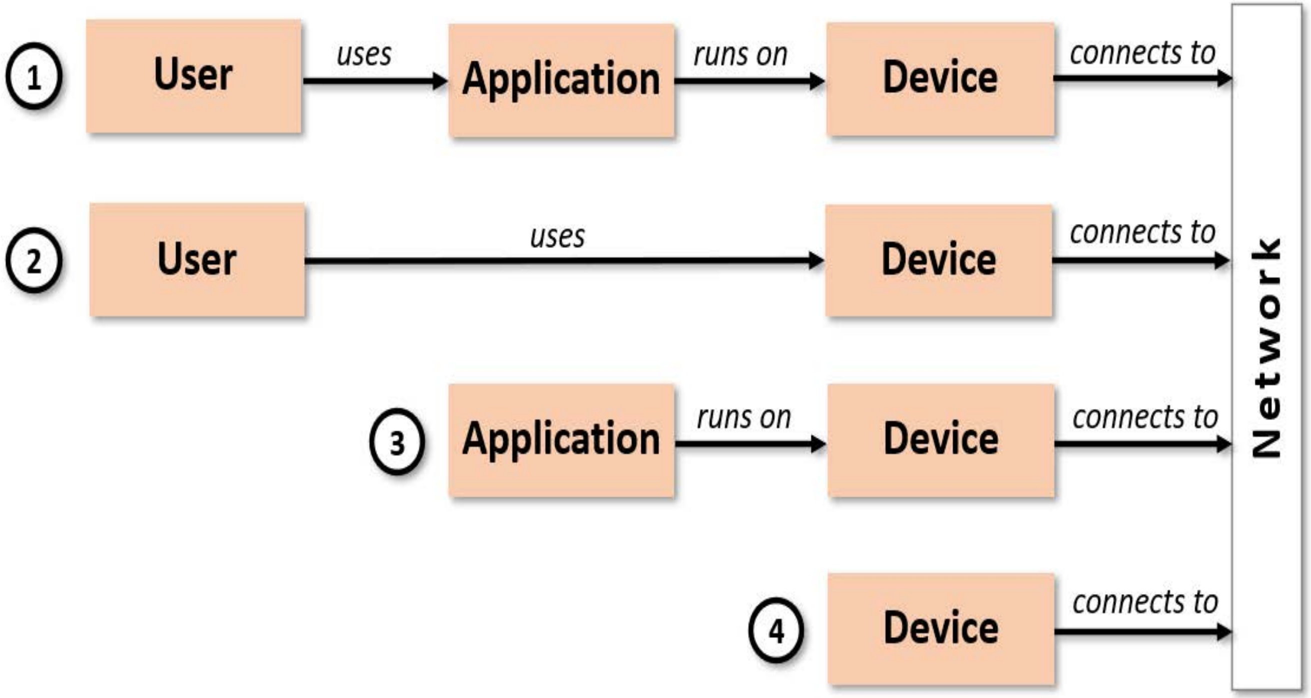
Policy End Points
- Policy Enforcement Point (PEP)
- Continuous Monitoring

Target Actors
- Users
- Devices
- Applications

Definition and Requirements

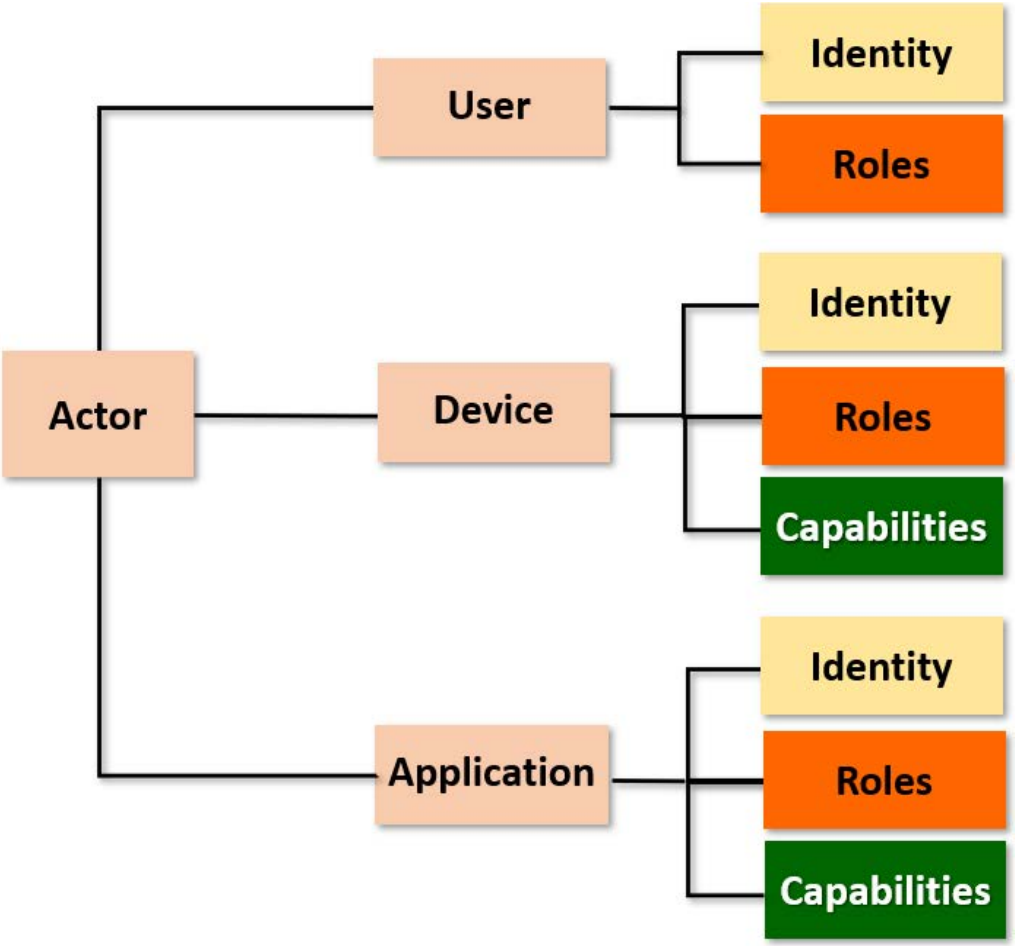
- Subject/Target Actor Types
  - Users, Devices, Applications
- Identity Service Attributes for:
  - Identity Provider (IdP), IdP Subscriber
  - Actors (Users, Devices, and Applications)
- Access Control Mechanisms
  - MAC, DAC, RBAC, ABAC
- Policy Management using PBAC for:
  - MAC, DAC, RBAC, ABAC, other AC mechanisms
- Continuous Monitoring
  - Time-based, Event-based, Data(ML)-Driven
- Policy Endpoint
  - Enforcement & Monitoring of Policies

Actor Types and Relationships Definitions



1. User using one or more Application running on a Device
2. User using a Device running a single application
3. One or more Applications operating autonomously on a Device
4. Single Application running on a Device

Actor Identity, Role and Capability Service Attributes, Parameters and Values for each Actor Type



Actor

User

Identity

Roles

Device

Identity

Roles

Capabilities

Application

Identity

Roles

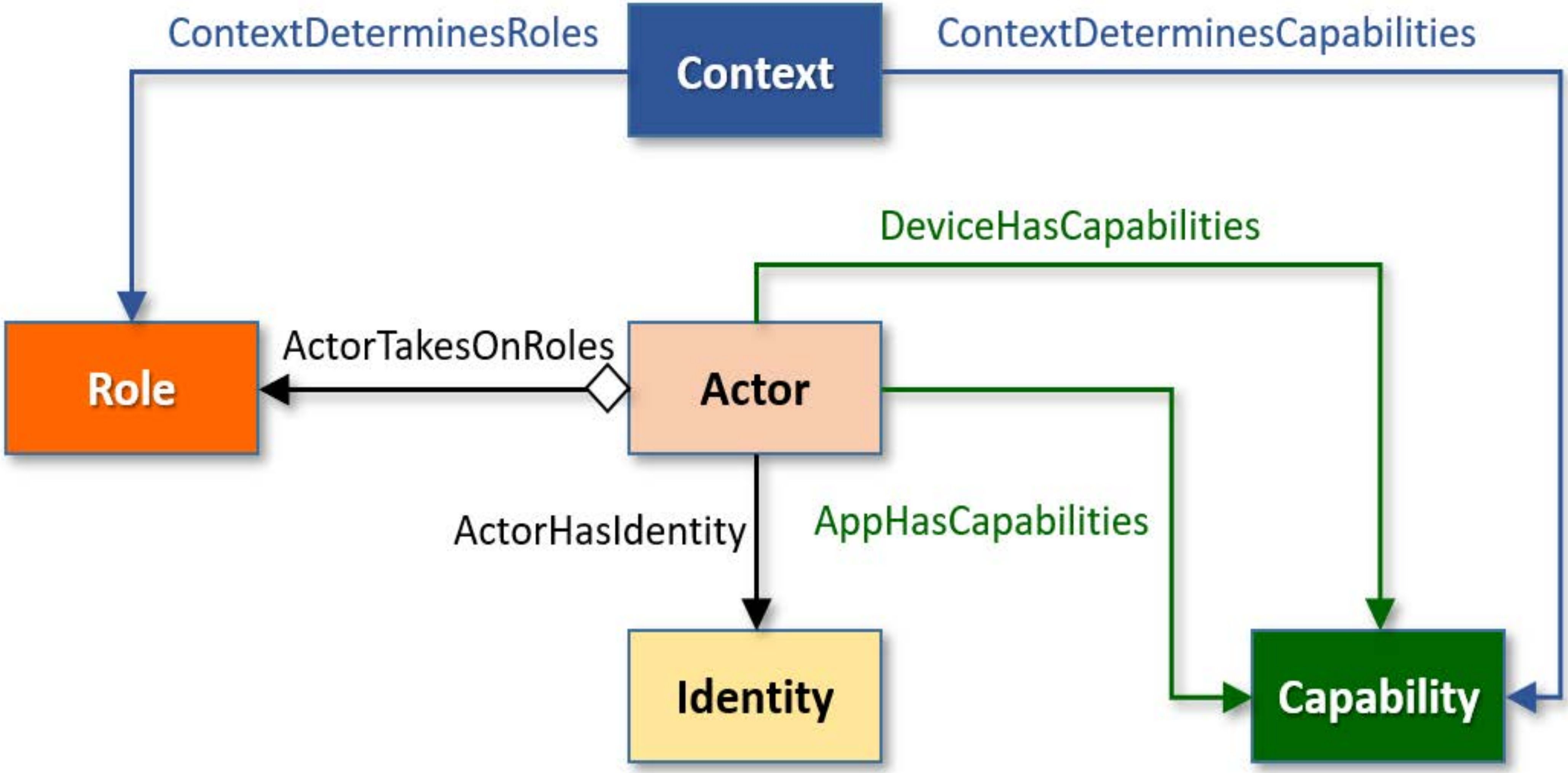
Capabilities

User Identity Service Attribute

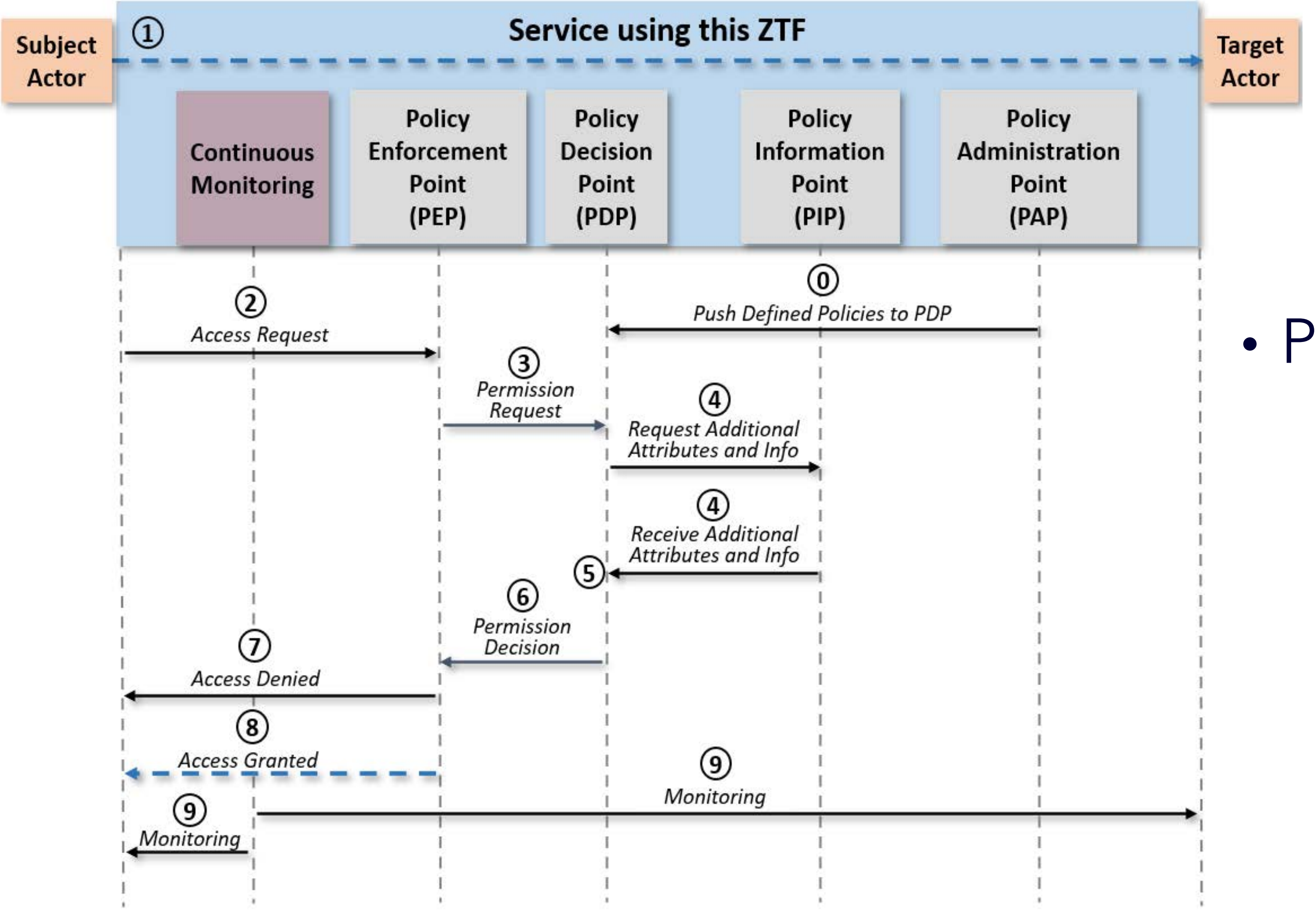
Parameters	Summary Description	Example Values
UserID	Unique string for the User	52688-2e93
UserCommonName	Human-readable name of the User, associated with the UserID	John Smith
UserName	Human-readable identity of the User associated with the UserID	jsmith
UserCredentialType	Type of identity credentials of the User requesting authentication	sha3{concat(UserName+password)}, biometric identifier

```
{"UserIdentityServiceAttribute":[
  { "UserID":"2e93-95e4" },
  { "UserCommonName":"John Smith" },
  { "UserName":"jsmith" },
  { "UserCredentialType":" certificate" }
]}
```

Actor Identity, Role, Capability and Context Relationships



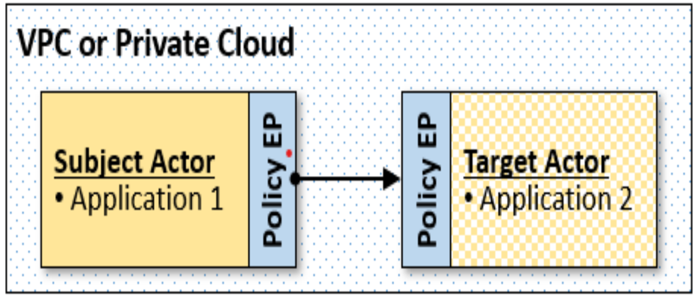
Definition of Policy Functions that affect Subject and Target Actors



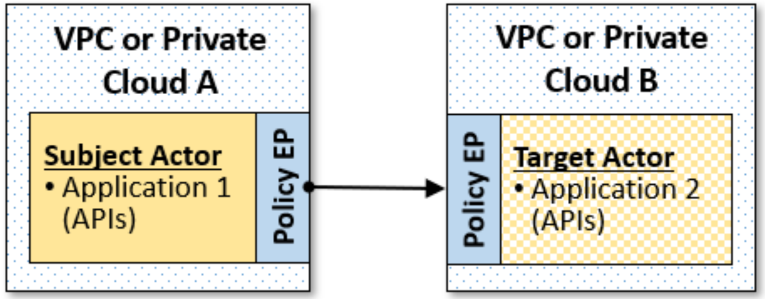
Subject Actor
①
Service using this ZTF
Target Actor
Continuous Monitoring
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Policy Information Point (PIP)
Policy Administration Point (PAP)
⓪
Push Defined Policies to PDP
②
Access Request
③
Permission Request
④
Request Additional Attributes and Info
④
Receive Additional Attributes and Info
⑤
⑥
Permission Decision
⑦
Access Denied
⑧
Access Granted
⑨
Monitoring
⑨
Monitoring

- Policy Functions
  - Policy Enforcement Point (PEP)
  - Policy Decision Point (PDP)
  - Policy Information Point (PIP)
  - Policy Administration Point (PAP)

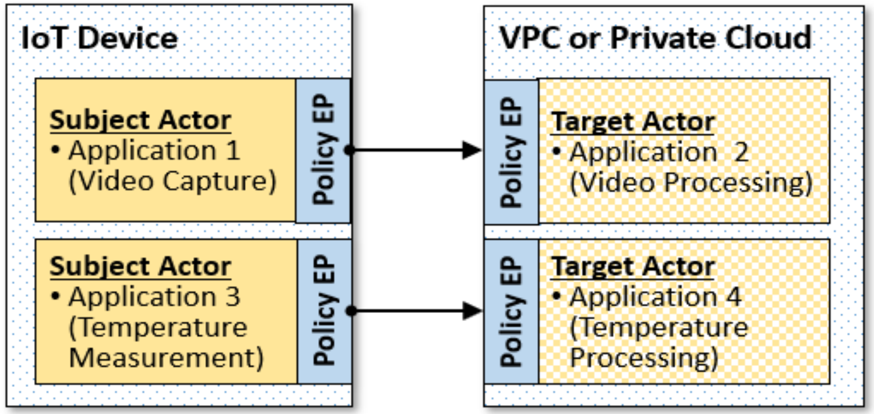
Informative Use Cases for Policy Endpoint (EP) Placement



EP for Apps in a Cloud

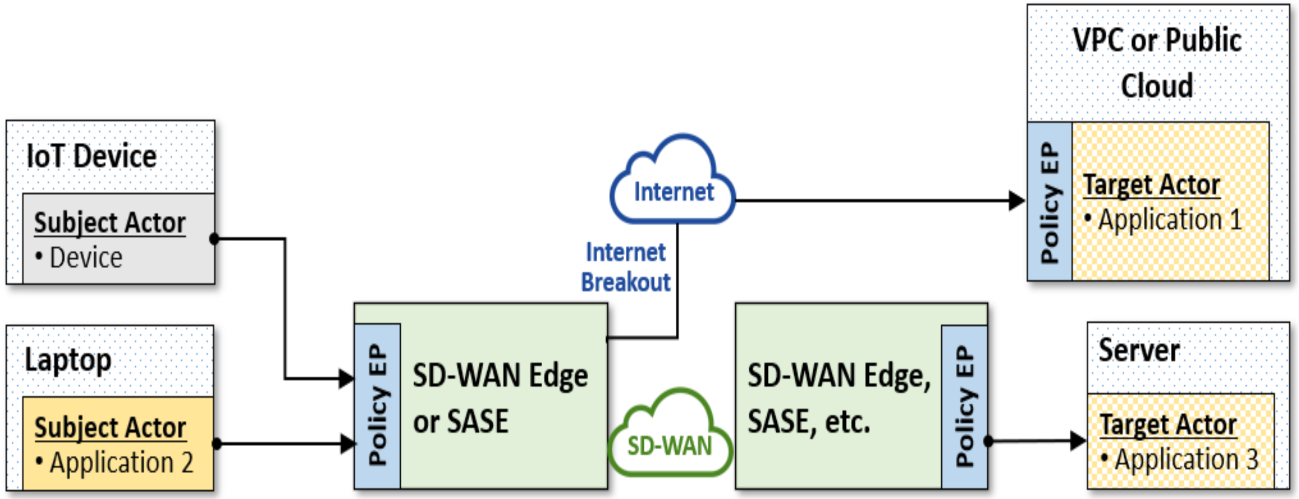


EP for Apps in different Clouds

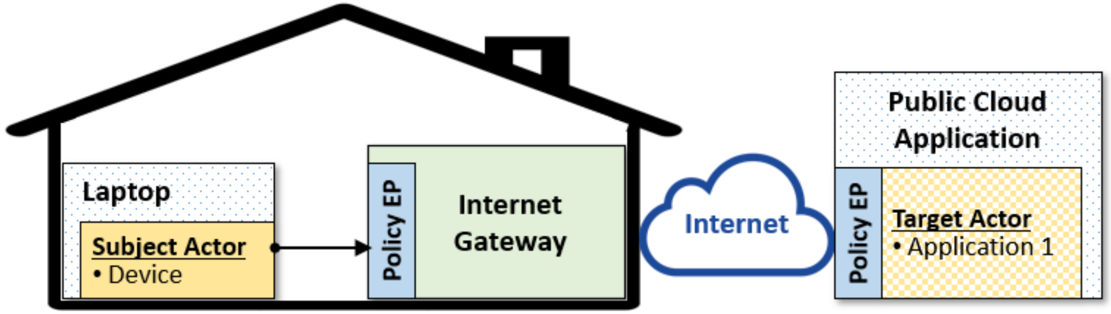


IoT Device
Subject Actor
• Application 1 (Video Capture)
Policy EP
Subject Actor
• Application 3 (Temperature Measurement)
Policy EP
VPC or Private Cloud
Policy EP
Target Actor
• Application 2 (Video Processing)
Policy EP
Target Actor
• Application 4 (Temperature Processing)

EP for Apps on a Device and for Apps in Cloud

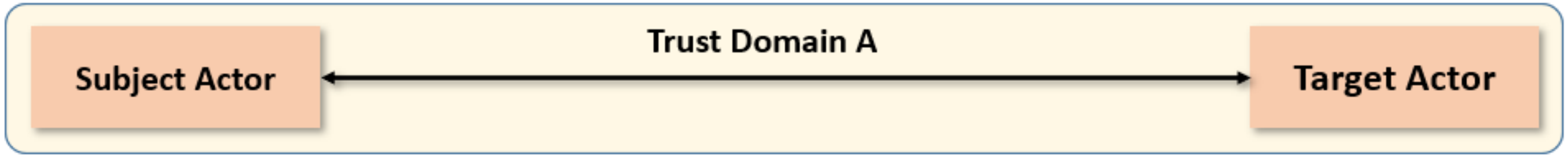


EP on SD-WAN Edge or SASE Device and for App in Cloud

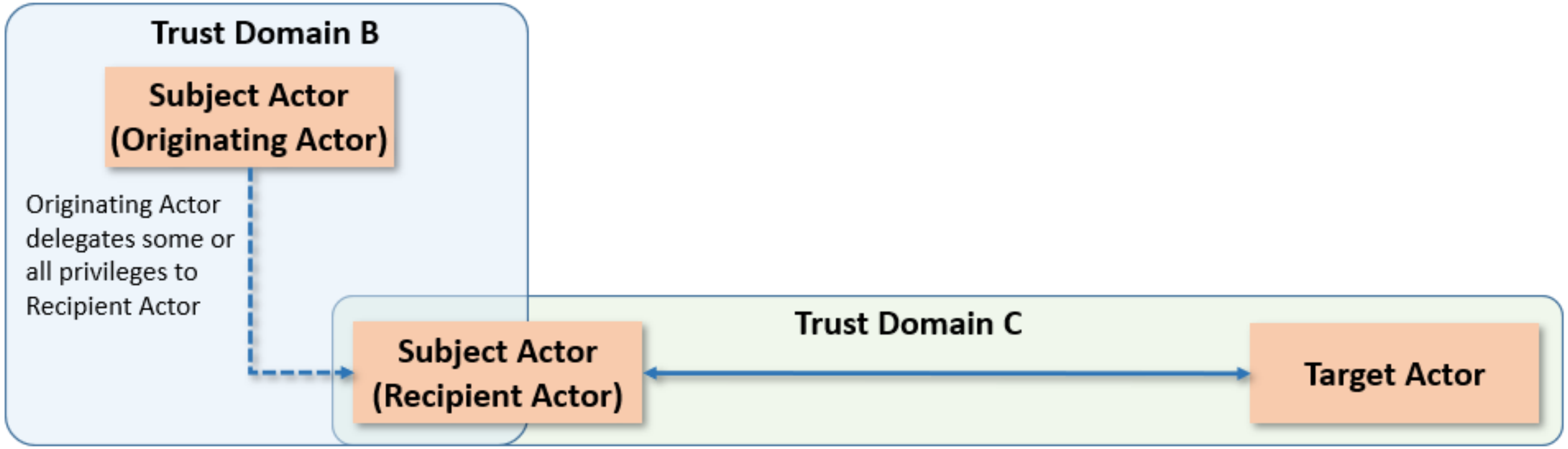


EP on Internet Gateway Device and for App in Cloud

Informative Appendix Describing Actor Delegation and Trust Domain Membership



1. No Delegation


Trust Domain B
Subject Actor (Originating Actor)
Originating Actor delegates some or all privileges to Recipient Actor
Trust Domain C
Subject Actor (Recipient Actor)
Target Actor

2. Subject Actor (Originating Actor) Delegates Privileges to Recipient Actor

MEF 3.0 SASE Services

July 2023

MEF

Industry Opportunities for SASE

1 Network security architectures that place the enterprise data center at the center of connectivity requirements are an inhibitor to the dynamic access requirements of digital business.

2 Digital business and edge computing have inverted access requirements, with more users, devices, applications, services and data located outside of an enterprise than inside.

3 Complexity, latency, and the need to decrypt and inspect encrypted traffic once will increase demand for consolidation of networking and cybersecurity capabilities into a cloud-delivering model.

4 To provide low-latency access to users, devices, and cloud services anywhere, enterprises need SASE offerings with a worldwide fabric of POPs and peering relationships.

Solving Industry Challenges for SASE & Zero Trust MEF SASE 117 & MEF Zero Trust 118

A secure, managed, cloud-based SASE service with Zero Trust principles

A clear industry SASE service definition. Ability to **compare apples to apples** with service offerings.

- MEF provides the framework, vocabulary, constructs, labels and service attributes
- MEF provides a Zero Trust framework to be used by SASE

MEF third-party certification (in development) which **provides confidence** of a SASE service

How MEF Solves the Challenges

Provide Common Language

Enable a wide range of ecosystem stakeholders to use the same terminology when buying, selling, assessing, deploying, and delivering SD-WAN SASE & ZT services

Ensure Service Resiliency

Make it easier to interface policy with intelligent underlay connectivity services to provide a better end-to-end application experience with assured service resiliency

Orchestrate Services across Automated Networks

MEF standardized LSO APIs orchestrate SD-WAN, SASE & ZT services

Certify Services

Certified MEF SD-WAN & SASE offerings ensure confidence that a service meets a fundamental set of requirements

MEF SASE Service Attributes and Service Framework MEF 117

MEF SASE 117 and Zero Trust Framework 118 Official Industry Standards

MEF

Standard

MEF 117

SASE Service Attributes and Service Framework

MEF

Standard

MEF 118

Zero Trust Framework for MEF Services

Secure Access Service Edge (SASE) MEF 117

SD-WAN

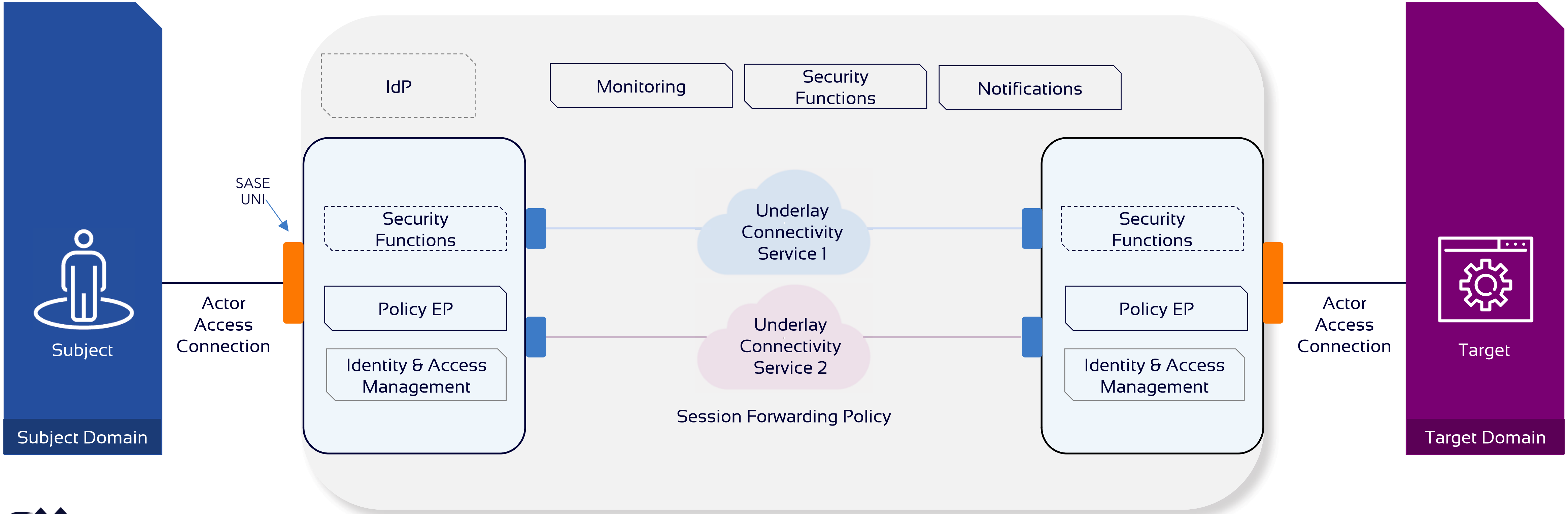
- Policy
- Secure Access from Anywhere with any Device
- VPN and overlay SD-WAN based
- WAN App Optimization and prioritization
- Thin CPE model

Cybersecurity

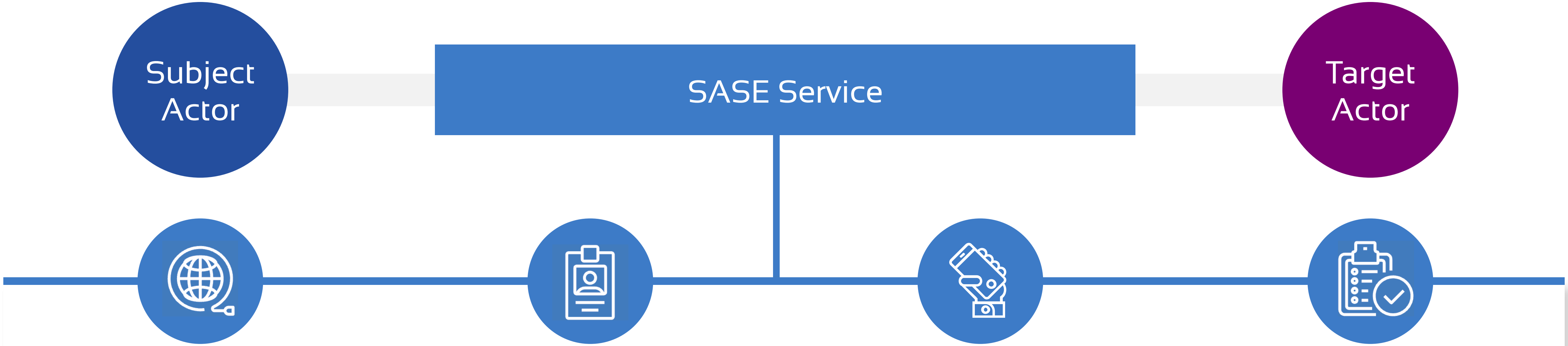
- Policy
- Security where needed (Cloud or on-premises)
- Zero Trust based
- Sites uses the secure cloud to get to the Internet, etc
- Scalable for multitenant
- Virtualized and cloud native

MEC Edge

- Designed for the MEC edge
- All MEC edges creates the service edge SASE cloud
- Connections to public and private clouds
- Connections to the Internet



SASE Concepts



Subject Actor

SASE Service

Target Actor

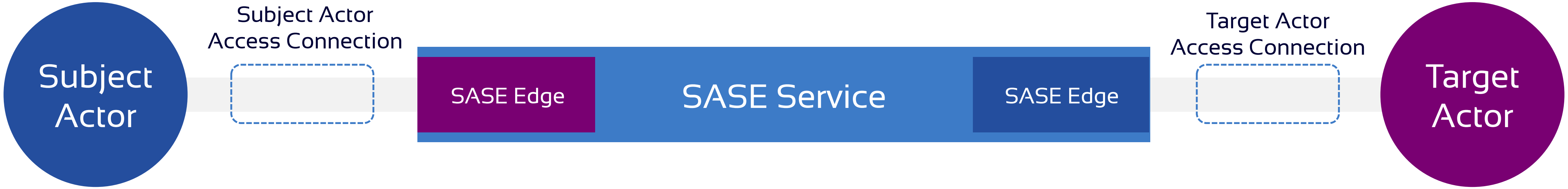
A SASE Service is a service that combines wide-area network connectivity and security functions to grant a Subject Actor access to a Target Actor for a given Session

Access is based on the Subject Actor’s Identity, Context, and Role in accordance with the performance criteria and Security Policies set by the SASE Service Subscriber

Actors are User, Device, or Application

Access to the SASE service is independent of location of the users, devices or applications and authorized according to Policies set by the Subscriber

Actor Access Connection


Subject Actor
Subject Actor Access Connection
SASE Edge
SASE Service
SASE Edge
Target Actor Access Connection
Target Actor

Actor Access Connections can be physically implemented in a variety of ways such as campus LAN, public wireless network, 5G, VXLAN, etc.
Actor Access Connections can be concatenations of implementations.

SASE Sessions

- A SASE Session, or “Session,” is a set of IP packets determined by a Session Specification and a State
- Each SASE Session has a unique identifier known as the *Session ID*

Session Specification

- Actor List
  - Subject
  - Target
- Application Flow Specification

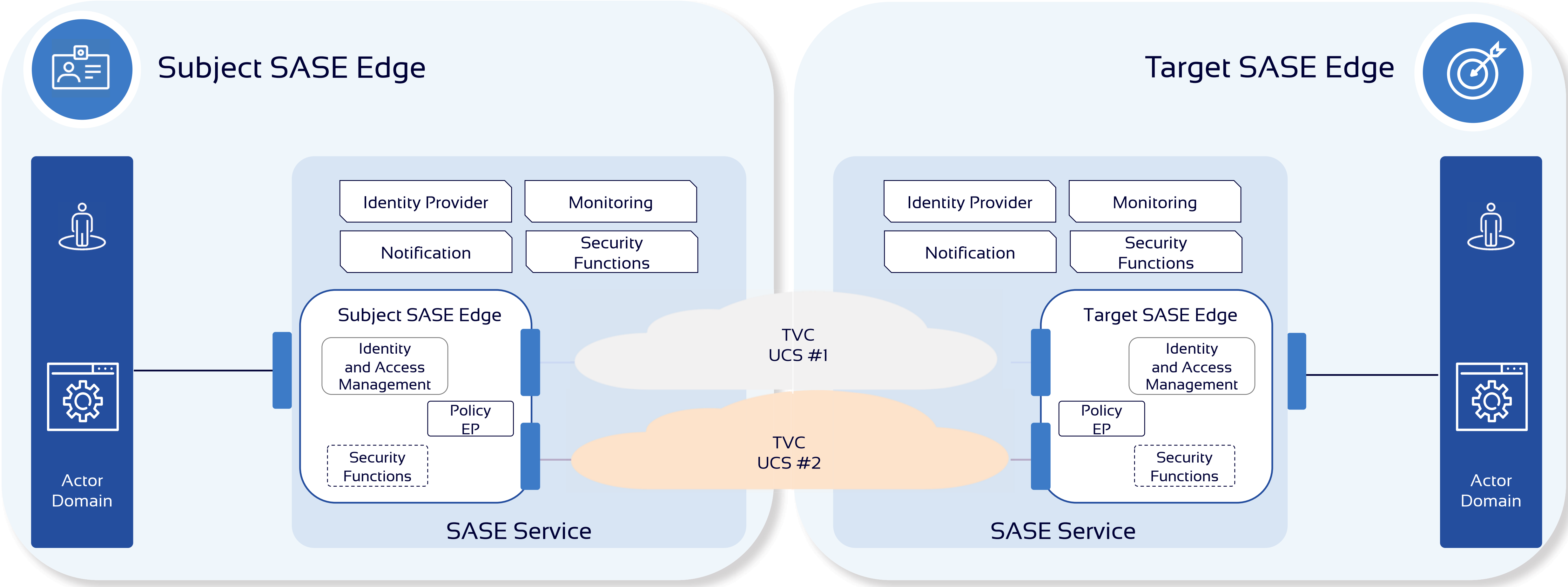
Session State

- Initial
- Operational
- Re-evaluate
- Terminal

SASE Policy

- Policy Criterion

SASE Service Edges



A Service Provider **SHOULD** support SD-WAN Service as defined in MEF 70.1 for the connectivity between SASE Edges.

Security Functions

A SASE Service delivers and manages cloud-native security functions as specified by the SASE Subscriber Policy for a specific session

Atomic Security Functions

- Middle Box Function (MBF)
- IP, Port and Protocol Filtering (IPPF)
- DNS Protocol Filtering (DPF)
- Domain Name Filtering (DNF)
- URL Filtering (URLF)
- Malware Detection and Removal (MD+R)

=

Vendor Defined Security Functions

- Cloud Access Security Brokers (CASB)
- Next Generation Firewalls (NGFW)
- Secure Web Gateway (SWG)
- Software Defined WAN (SD-WAN)
- Zero Trust Network Access (ZTNA)

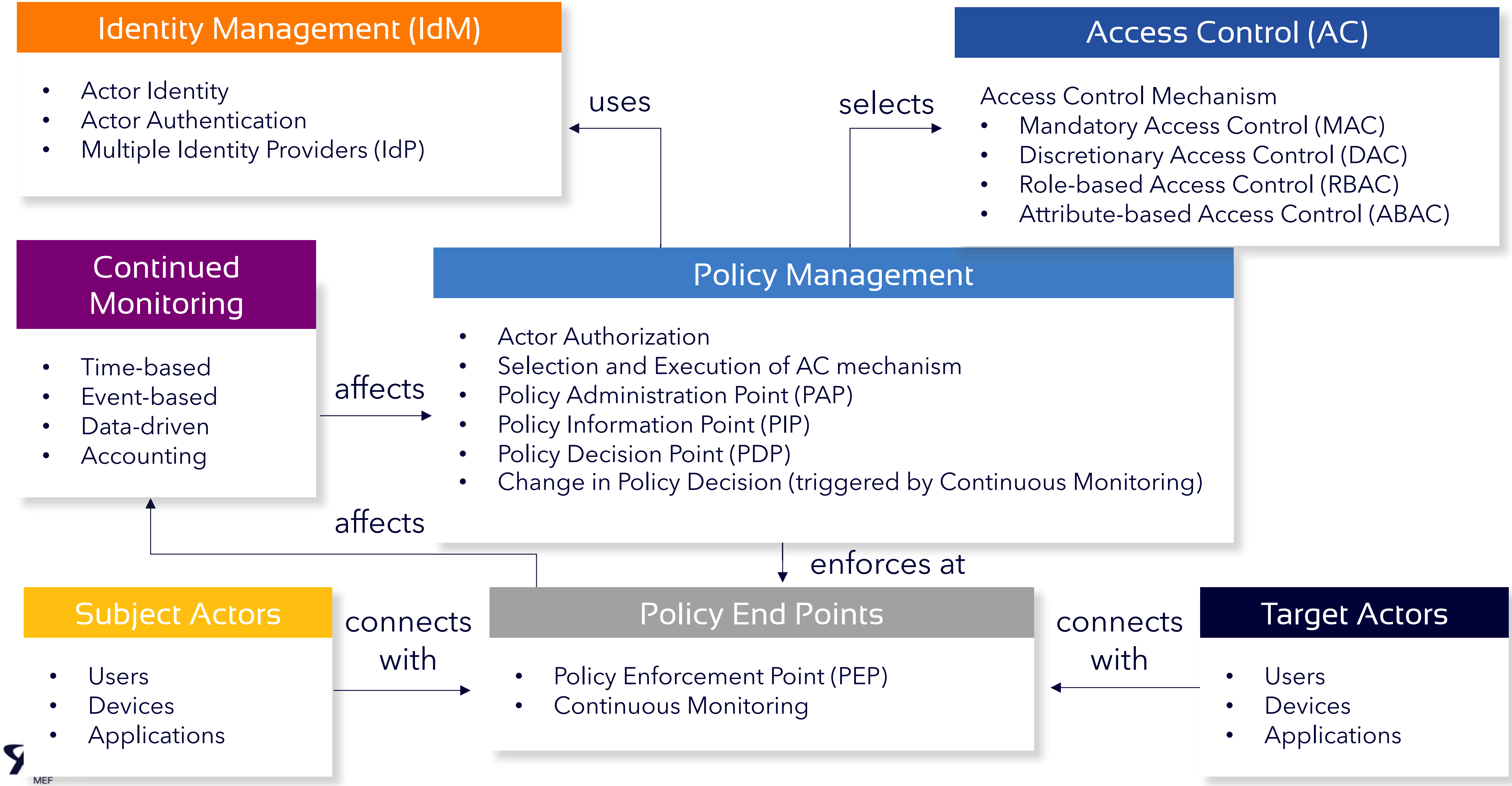
SASE Policies

A SASE Policy is a set of Policy Criteria, each of which is a set of conditions and/or constraints for which network and Security Functions will be applied between the authenticated Subject Actor & the Target Actor.

A SASE Policy MUST include the following Policy Criteria:

- Identity and Access Management Policy Attributes - is the set of Policy Criteria that are in order to properly authenticate the identity of a given Actor and to secure the Actor Access Connection
- Context Policy Attributes - is a set of parameters that influence the authorization of a given Session within a SASE Service (ex: time of day, location, etc.)
- Security Policy Attributes - is a set of Security Functions and their associated parameters
- Session Forwarding Policy Attributes - is a set of forwarding and performance requirements that influence how a given Session traverses the SASE Service
- Monitoring Policy Attributes - is a set of continual evaluation requirements that evaluates the SASE Policy attributes for changes, triggers Session State Changes, and subsequent SASE Policy selection for a given Session as it traverses the SASE Service
- Notification Policy Attributes – is a set of notification requirements that controls the alerts and communications sent to the Subscriber by the SASE Service.

SASE Incorporates a Zero Trust Framework from MEF 118



Identity Management (IdM)

- Actor Identity
- Actor Authentication
- Multiple Identity Providers (IdP)

Access Control (AC)

Access Control Mechanism

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-based Access Control (RBAC)
- Attribute-based Access Control (ABAC)

Continued Monitoring

- Time-based
- Event-based
- Data-driven
- Accounting

Policy Management

- Actor Authorization
- Selection and Execution of AC mechanism
- Policy Administration Point (PAP)
- Policy Information Point (PIP)
- Policy Decision Point (PDP)
- Change in Policy Decision (triggered by Continuous Monitoring)

Subject Actors

- Users
- Devices
- Applications

Policy End Points

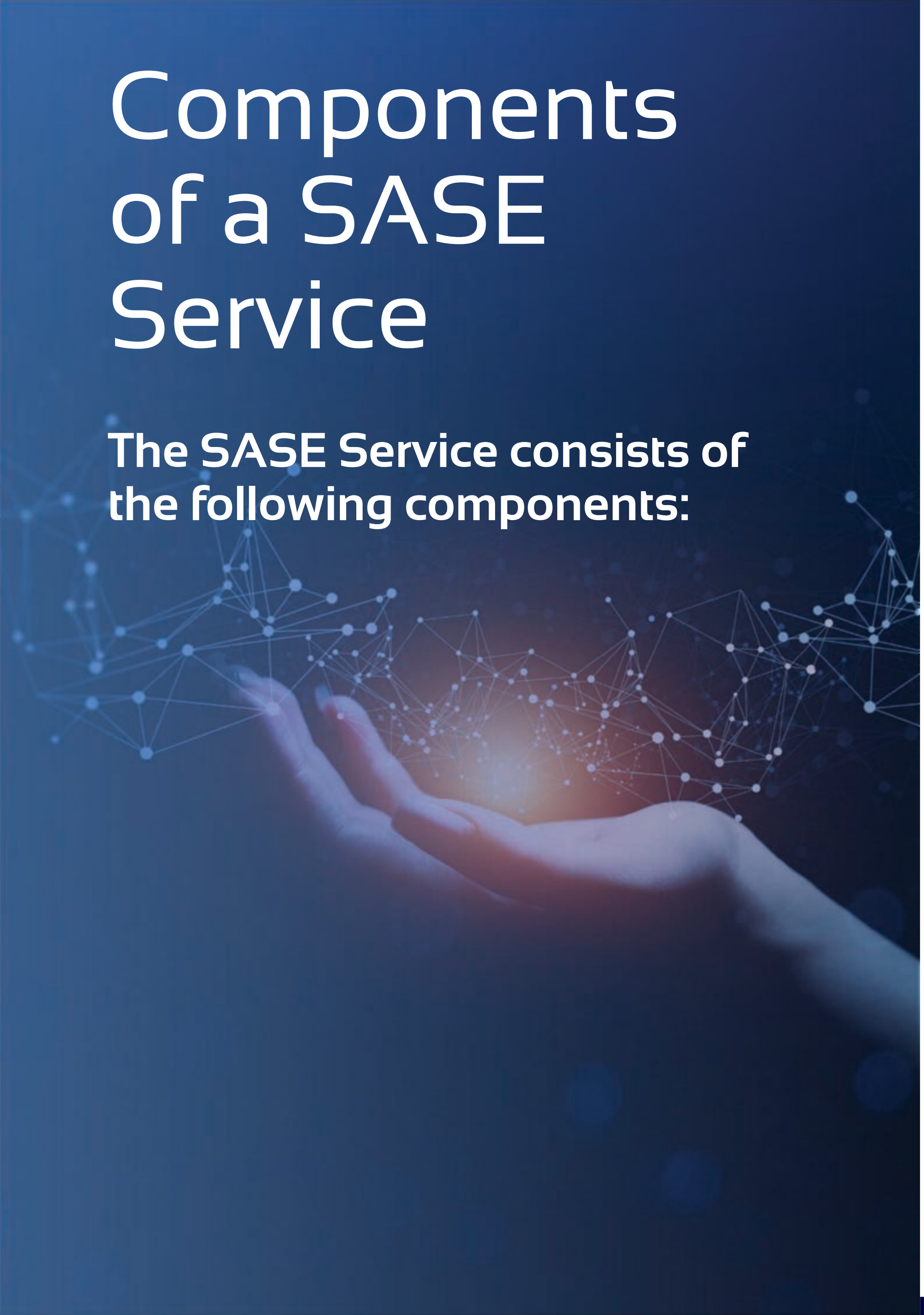
- Policy Enforcement Point (PEP)
- Continuous Monitoring

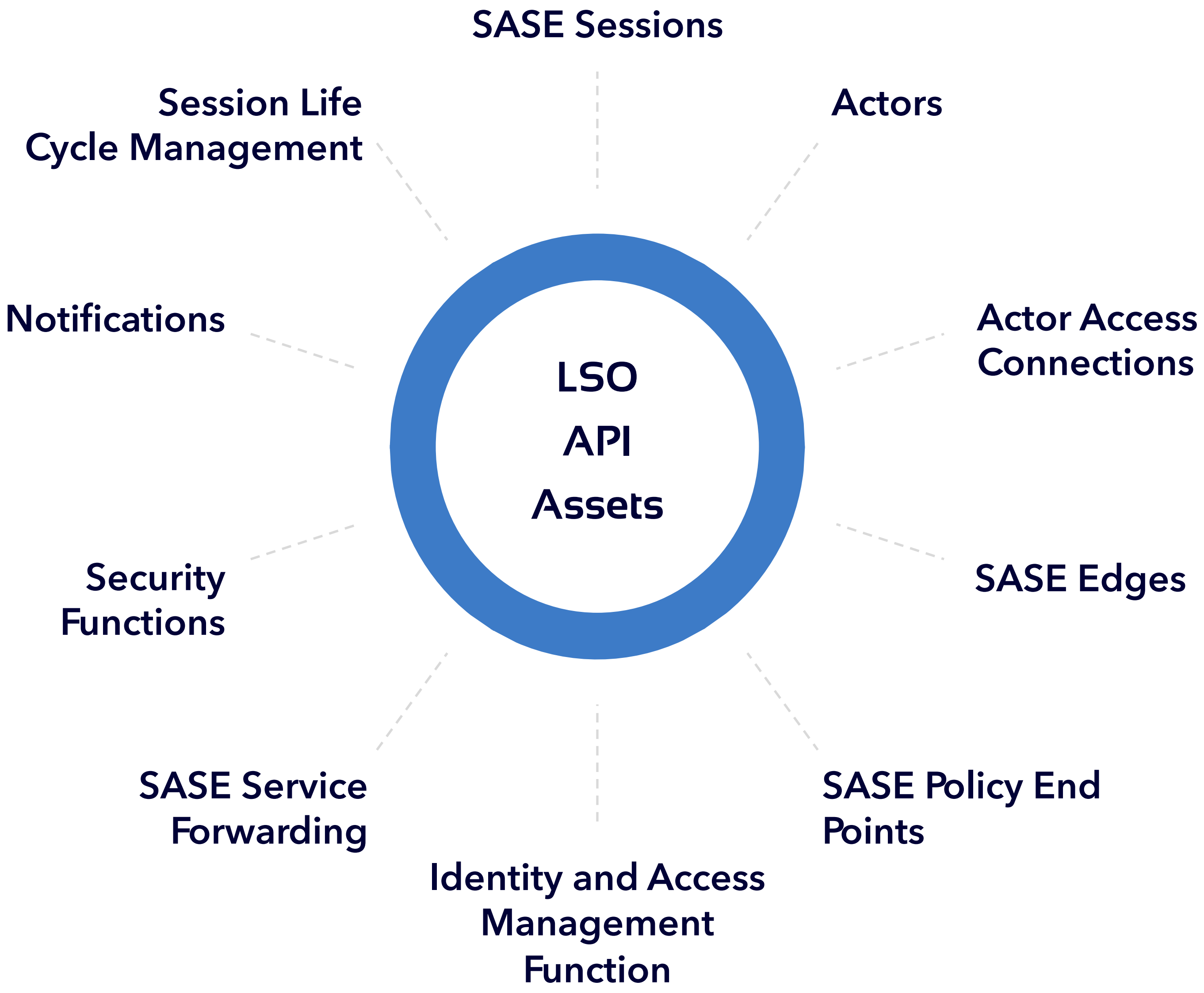
Target Actors

- Users
- Devices
- Applications

Components of a SASE Service

The SASE Service consists of the following components:





LSO API Assets

SASE Sessions

Actors

Actor Access Connections

SASE Edges

SASE Policy End Points

Identity and Access Management Function

SASE Service Forwarding

Security Functions

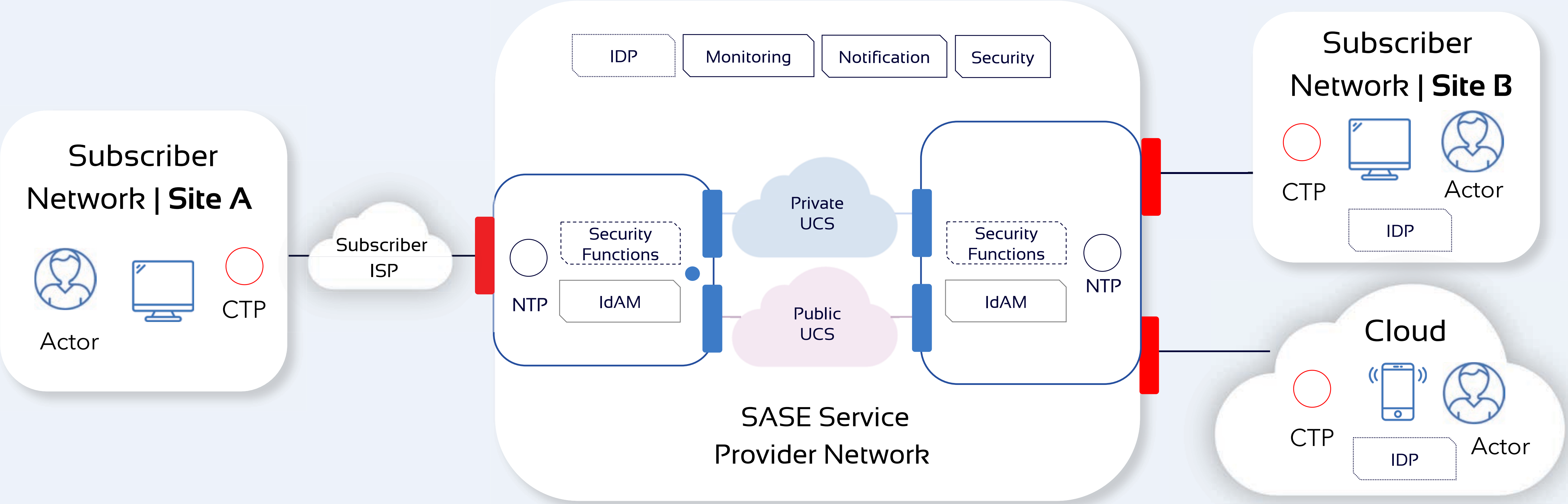
Notifications

Session Life Cycle Management

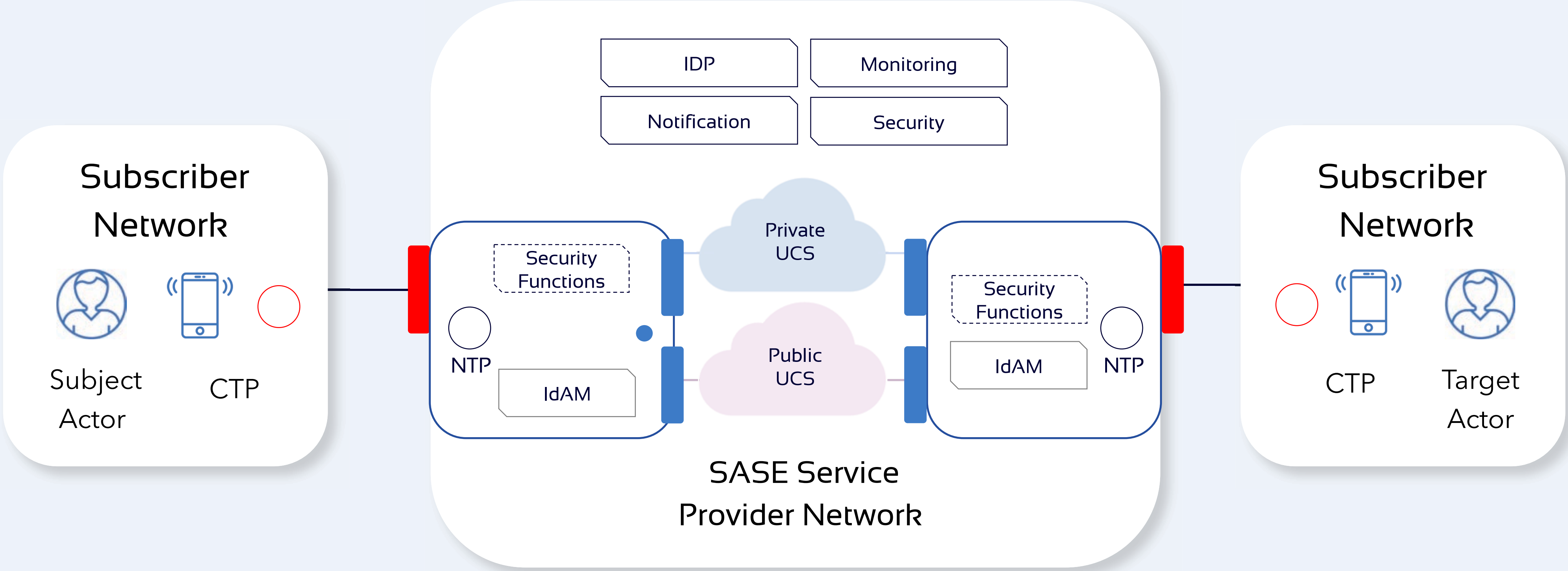
SASE Service Use Cases

USE CASE #1

Generic SASE Service

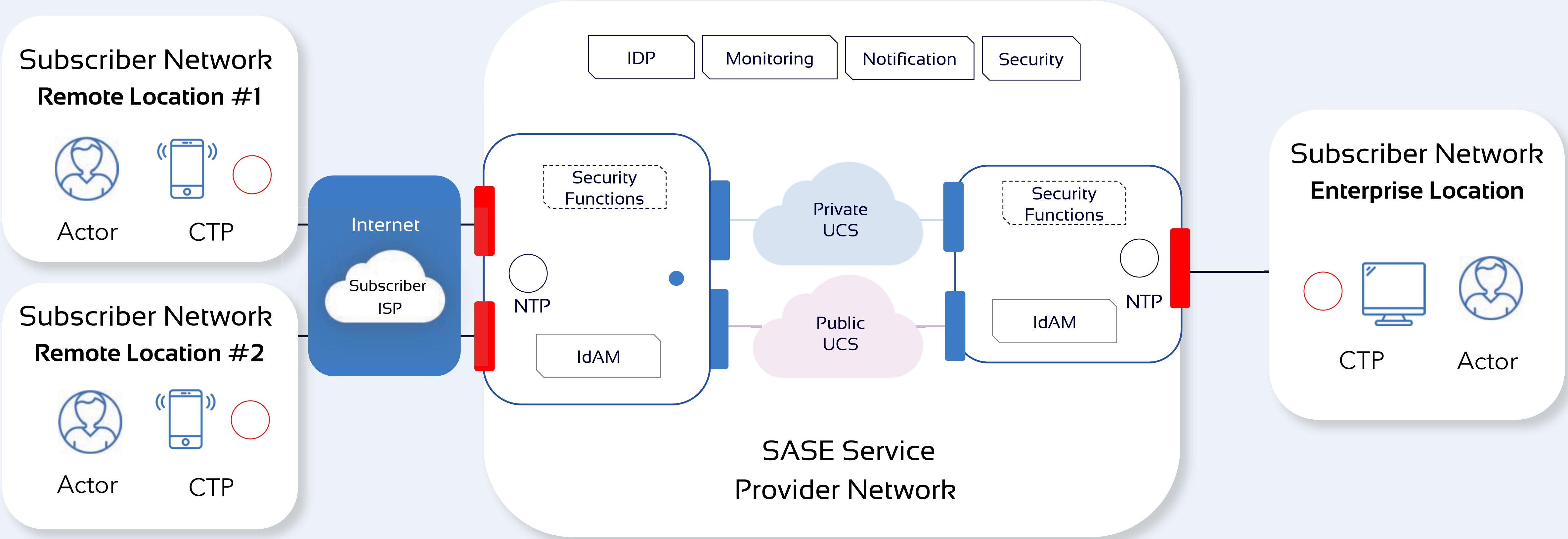


SASE: On-Premises



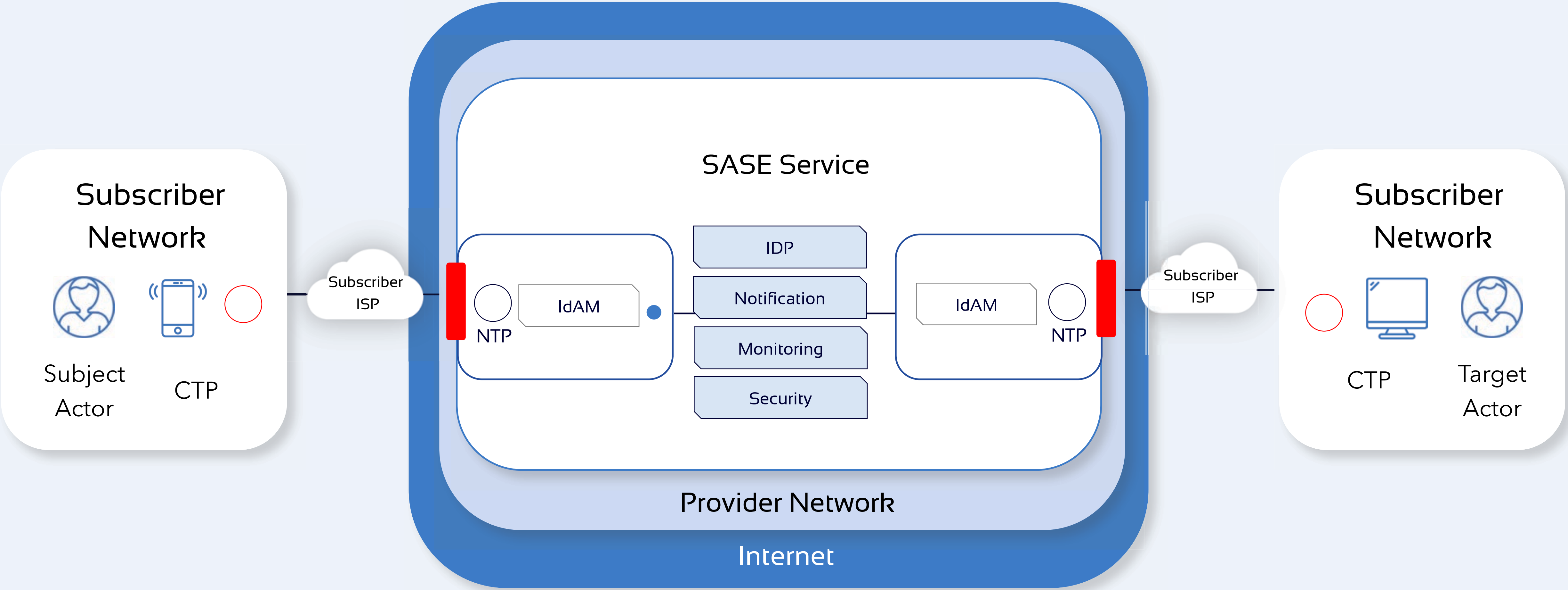
USE CASE #3

SASE: Remote Access



USE CASE #4

SASE: Cloud-delivered Service



Call to Action & MEF Resources

Summary

MEF 117 provides a service definition that integrates both Security and Networking constructs, that is driven by policy, and that adopts a Zero-Trust Framework.

- Integrated Security and Networking
- Policy-Driven
- Zero Trust

Business Call to Action

- Get involved in next version of MEF SASE and Zero Trust Framework (must be a MEF member)
- Request in RFPs/RFIs for SASE service providers and vendors to comply to MEF 117 SASE standard
- Request in RFPs/RFIs for SASE service providers and vendors to be MEF SASE certified (coming soon)
- Social media with MEF to create SASE market awareness for the industry

SASE Resources to Get Started

- Download the standards:
- Visit: MEF.net/SASE
- SD-WAN & SASE Research Tracker
- SASE SD-WAN North Star
- Video: Tackling SD-WAN and SASE Managed Service Provider Challenges
- FAQ: MEF 3.0 SD-WAN & SASE
- SD-WAN & SASE News Articles
- MEF Executives at the Edge Podcast

MEF Edge VIEW Blog: SD-WAN & SASE, Cybersecurity

MEF.net/SASE

MEF
FREE DOWNLOAD
MEF SD-WAN & SASE Market Brief
Tackling SD-WAN and SASE Managed Service Provider Challenges
DOWNLOAD NOW

Tackling SD-WAN and SASE Managed Service Provider Challenges
WATCH NOW
MEF
STAN HUBBARD
Principal Analyst

MEF SASE & SD-WAN New Standards

Work in Progress

Moderator: Chris Purdy
VP Product Management, Canoga Perkins
DSC Co-Chair

Spotlight on SASE
19 July 2023

Presenters

Neil Danilowicz

Principal Architect, Versa Networks

Mike Bencheck

MEF Fellow, MEF Editor at large

Vik Phatak

Chairman and CEO
CyberRatings.org

Agenda

- Part 1: Overview of Work in Progress (45 mins)
  - Approved Projects
    - SD-WAN Certification Phase 2 (W90.2) – Mike
    - SSE and Zero Trust Test and Certification Requirements (W162 & W163) – Mike
    - Universal SD-WAN Edge (W119) – Mike
    - Security Functions for IP Based Services (W138) – Neil
  - Incubation Groups
    - Evolution of MEF SASE Service Attributes Service Framework (W117.1) – Neil
    - Evolution of Zero Trust Framework (W118.1) – Neil
    - Secure Service Edge (SSE) Attributes – Mike
- Part 2: Round Table discussion on the value of this work (15 mins)

SD-WAN Certification Phase 2 (W90.2)

MEF

Spotlight on SASE
19 July 2023

Scope

The scope of this document defines the requirements for testing to obtain a rating of either an SD-WAN Edge Vendor offering or an SD-WAN Service Provider offering. This rating is provided after completion of testing by a 3rd party (Cyber Ratings). The testing will include the following areas:

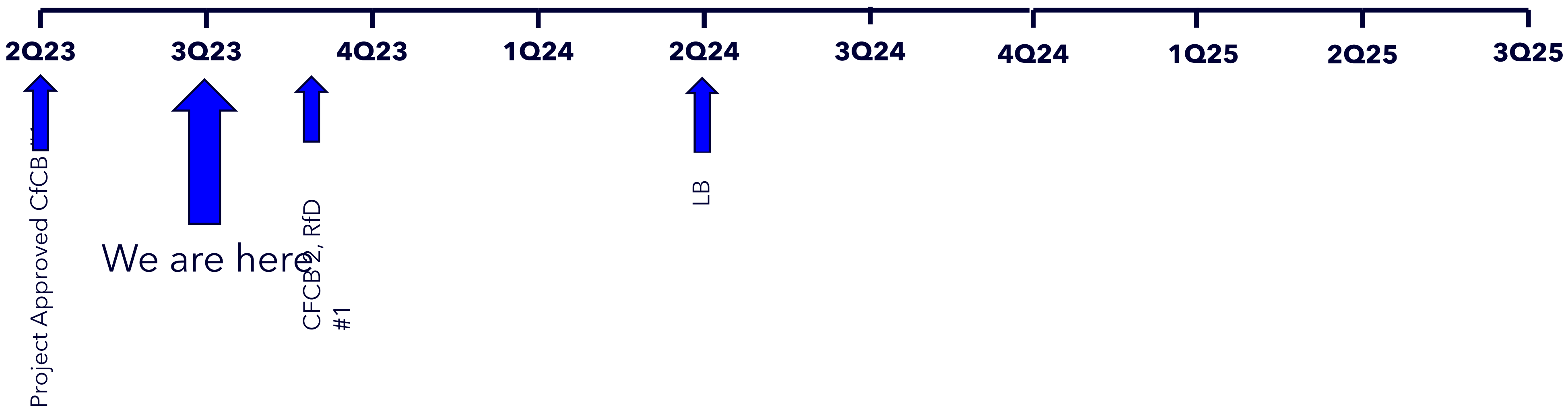
- MEF 70.1 terminology integration
- Application Flow Forwarding and Policy Testing (MEF 70.1)
- Application Flow Forwarding and Policy Testing over impaired UCSs of an SWVC
- SD-WAN Edge and SWVC Performance
- SD-WAN and SWVC Stability and Reliability
- Cost of rating

Each of these will be detailed with appropriate test steps and methodologies defined within the document.

Current Status

- CfC #1 closed 10 July
  - 52 comments received from 4 commentors
    - Versa
    - Bell Canada
    - Cisco
    - CyberRatings
  - 24 Technical
  - 10 T/E
  - 18 Editorial
- On-going discussion on the need for clarification and need of the current tests

Schedule


2Q23
3Q23
4Q23
1Q24
2Q24
3Q24
4Q24
1Q25
2Q25
3Q25
Project Approved CfCB #1
We are here
CFCB 2, RfD #1
LB

SSE and Zero Trust Certification Requirements (W162 & W163)

MEF

Spotlight on SASE

19 July 2023

Scope of SSE Deliverable from Project Proposal

The areas that are tested and included in the scope of the SSE document are:

- MEF Terminology (MEF 117)
- SSE Description
- Routing Functionality
- SSL/TLS Support
- HTTP and HTTPS Performance
- Reporting Capabilities (Security Event)
- Cloud Access/Application control (Multi-cloud how is this addressed)
- Threat Prevention
- Evasions

Scope of ZT Deliverable from Project Proposal

The areas that are tested and included in the scope of the ZT document are:

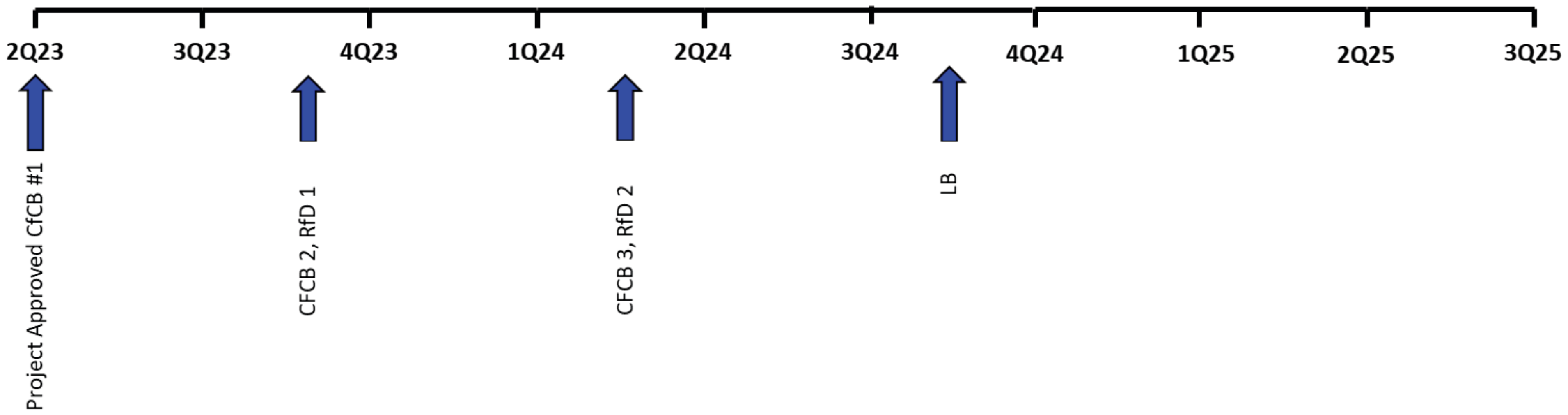
- MEF Terminology (MEF 118)
- ZT Description
- Policy Enforcement
- Reporting Capabilities (Security Event)
- Cloud Access/Application control (Multi-cloud how is this addressed)

Project Status

- MEF W162 and MEF W163 both completed first CfC
  - CfC opened 8 May
  - CfC closed 23 June
- MEF W162 received 161 Comments
  - 98 technical
  - 42 technical and editorial
  - 21 editorial
- MEF W163 received 137 Comments
  - 79 technical
  - 36 technical and editorial
  - 22 editorial

Schedule

SSE



2Q23 3Q23 4Q23 1Q24 2Q24 3Q24 4Q24 1Q25 2Q25 3Q25

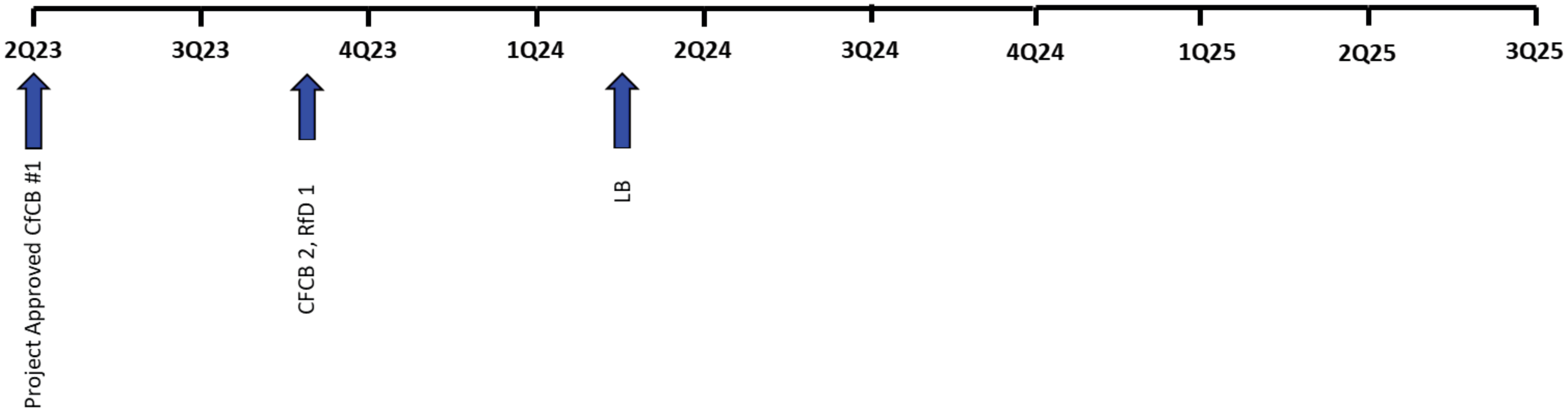
Project Approved CfCB #1

CFCB 2, RfD 1

CFCB 3, RfD 2

LB

ZT



2Q23 3Q23 4Q23 1Q24 2Q24 3Q24 4Q24 1Q25 2Q25 3Q25

Project Approved CfCB #1

CFCB 2, RfD 1

LB

Universal SD-WAN Edge (W119)

Spotlight on SASE
19 July 2023

Scope and Deliverables

This project will develop a MEF Standard that describes an implementation agreement for a Universal SD-WAN Edge capability that can be implemented in multiple vendors' SD-WAN Edge devices and also as a virtual network function (VNF). The Universal SD-WAN Edge describes a minimum set of functions and capabilities for the SD-WAN Data, Control, Telemetry, and Management planes that will enable Interoperability between a Universal SD-WAN Edge and vendor equipment. It is not a goal to enable interoperability between different vendors' SD-WAN Edge devices although that might be a result, but in any case, this interoperability would, in effect, represent a minimum common denominator of SD-WAN functionality.

This effort will use existing specifications and standards for the data, control, and management planes and will not define new protocols or APIs. Functions in scope:

1. Interoperable encrypted data plane
   - IP Transport only in v1
   - Encryption methods and algorithms
   - Cipher choices
   - Keys and certificates, authentication, and authorization e. Packet formats and metadata
   - Quality of Service
2. Interoperable control plane
   - Distribution of Subscriber Routes across SD-WAN Network
   - Agreement on IP routing options
   - Security Management
3. Interoperable management plane and performance management
   - Configuration of Universal SD-WAN Edge
   - Device monitoring/health/status
   - Deployment of Policies, Application Flow definitions, Zone definitions, Virtual Topology definitions (standardized structures /definition formats)
   - Assignment of Policies to Application Flows / Zones
   - Telemetry (may be in control plane)
   - Performance Monitoring (MEF 105)
   - Threshold Crossing Alerts (MEF 105)
   - Service Readiness Testing (SRT ala MEF 105)

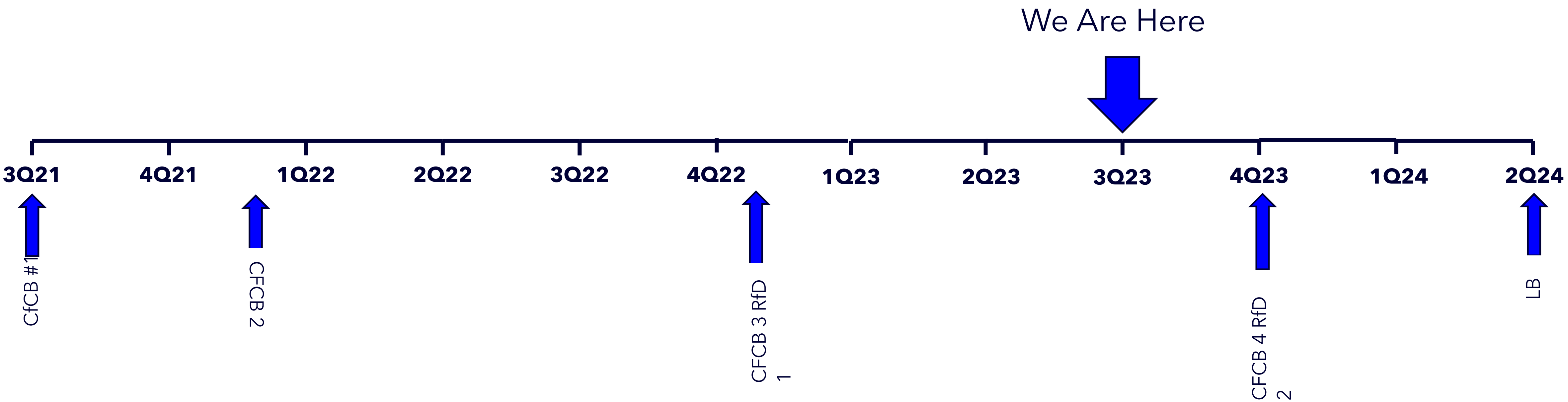
Universal SD-WAN Edge

- The Universal SD-WAN Edge supports a minimal set of data plane, control plane, management plane, and telemetry functions.
- The goal is to define an SD-WAN Edge that enables minimal SD-WAN interoperability with SD-WAN Services from multiple SD-WAN vendors.
- Typically located at a hub/cloud (aggregation) locations to access software functions, services, and resources.
- Uses existing SDO standards (i.e., not creating new protocols)
- Retitled document to "Universal SD-WAN Edge Implementation Agreement"

Key Areas of Interoperability

- Basic functions associated with:
  - Policy
    - Traffic Steering
    - Encryption
    - Performance
    - Etc.
  - Connectivity (data plane)
  - Routing (control plane)
  - Management (management plane)
  - Telemetry (management and/or control plane)

Schedule and Work Plan



Additional one quarter slip on CfC #4 and LB due to significant rewrite of the document

Security Functions for IP Based Services (W138)

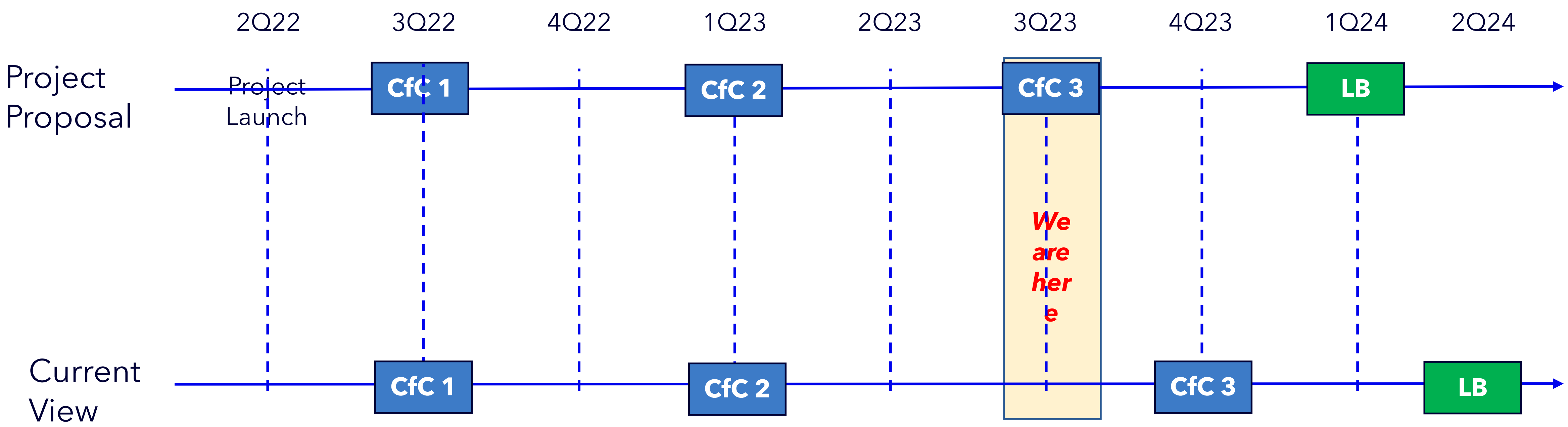
MEF

Spotlight on SASE
19 July 2023

Scope of Security Functions for IP Based Services (W138)

- Generalize the Security Functions specified in MEF 88 so that they are applicable to all IP-based Services…. Not just SD-WAN
  - Generalize Context
  - Generalize Security Policy Definition
  - Generalize Threat Model
  - Generalize Security Functions
  - Update Use Cases to cover examples beyond Security Functions over SD-WAN
- Enhance block/allow/quarantine lists based on threat intelligence and/or behavior such as continuous monitoring as specified in MEF 118
- Enhance middle-box security function to cover IPsec (vs just TLS)
- Add Notification Policy and Security Admin Notification (SAN) Policy
- Add Secure DNS Proxy security function
- Add Data Loss Prevention (DLP) security function

Project Schedule for MEF W138



Evolution of SASE Service Attributes and Service Framework (W117.1)

MEF

Spotlight on SASE

19 July 2023

SASE Evolution Project Scope

1. Enhance / improve the set of Security Functions
    - Data Loss Prevention (DLP).
        - Currently being developed in MEF W138.
    - Protective DNS (PDNS)
        - Currently being developed in MEF W138.
    - Remote Browser Isolation (RBI)
    - Cloud Access Security Broker (CASB)
        - Break into atomic components
            - Application Identity Management Function
                - This is similar to the current IDMF, but on an application basis and concerned more with the Cloud than the SASE Service itself
            - Gateway Function
                - In-line proxy
                    - Forward proxy
                    - Reverse proxy
                - Out of Band
                    - Application control via APIs
    - Air Gap concept
        - Segmentation
        - Zero Trust Delegation
        - Trust Zones

SASE Evolution Project Scope (cont'd)

2. Enhance / improve the set of Session Forwarding characteristics
   - Review the Requirement for SD-WAN as Networking for SASE Service
   - Map SD-WAN Service Attributes to SASE Service Attributes (where applicable)
   - Enhance Forwarding Characteristics
     - Choice of UCS Type
     - Performance Metric
     - Security Characteristics effects on Forwarding characteristics
3. Add Use Cases
   - Multi-cloud Use case
   - Cloud to Cloud Use case
   - VPN replacement (ZTNA)
   - Cloud only Delivered SASE
     - o SSE use case
4. Enhance / improve the SASE concepts and requirements to align with MEF 118 Zero Trust Framework and MEF W118.1 revision project (provided it is approved)
   - Align with the Zero Trust Framework as currently written in MEF 118
     - Trust Delegation
     - Trust Domains
     - Identity Management
   - Align with enhancement to the above items resulting from the Zero Trust Framework Revision Project MEF W118.1 (if approved)

SASE Evolution Project Scope (cont'd)

5. Enhance / improve the set of Session Notification or Monitoring characteristics
   - Security Event Notifications
     - Enhance/Add parameters that are required or recommended to be included in the SSEN
   - Service Administration Notification
     - Enhance/Add parameters that are required or recommended to be included in the SSAN
   - Develop requirements, parameters, attributes around usage of SSEN and SSAN to 3rd Party AI/ML solutions
6. Add Threat Model
   - Utilize existing Threat Model(s) to demonstrate how SASE solves industry standard vulnerabilities and threats
7. Clarify language involving the use of the term Actor
   - The 2Q2023 Members Meeting provided language needed for the TCC to do certification work and was agreed to be added to the next revision to the SASE Service Attributes and Service Framework
8. Authorize the Project to consider a change to the name of the Service Definition
9. Correct errata
10. This project will result in a new Standard (MEF 117.1).
    - This resulting standard will supersede MEF 117

Project Schedule

- CfC 1 - Q1 2024
- CfC 2 - Q3 2024
- CfC 3 - Q1 2025
- Letter Ballot - Q3 2025

Evolution of Zero Trust Framework (W118.1)

MEF

Spotlight on SASE

19 July 2023

Scope of ZT Framework Evolution (W118.1)

- This project will result in a new Standard (MEF 118.1) which will supersede MEF 118
- Define auditing requirements to determine whether appropriate policy decisions/actions were taken in the appropriate policy management sections. Areas to consider include:
  - Proactive and reactive policy decisions/actions
  - Control and management plane decisions/actions
- Expand/Add informative use cases in existing informative appendix A or add new informative appendix if warranted.
  - Implementation guidance to speed deployment
- Create definition and requirements for visibility of each appropriate section of MEF 118, e.g., Subject Actors actively interacting with Target Actors, Actors that are authenticated, Actors that are monitored, etc.
  - Visibility could be GUI or "event notification" like a SEN/SAN.
- Create definition and requirements for Risk and Risk Score into existing MEF 118 risk section 16.3
  - Add how a risk score gets input into MEF 118 Continuous Monitoring section 17
    - Risk score obtained from external feeds or applications (risk score could be different for different verticals) that may result in a change in policy enforcement, e.g., new policy is applied that could block (event-based)
  - Define threshold mechanisms, e.g., risk levels are used (green, yellow, red), which would have thresholds for separating them and could trigger an event
- Clarify language involving the use of the term Actor
  - The 2Q2023 Members Meeting, additional informative text was agreed to be added to address questions regarding Actor and Threat Actor from the TCC
- Correct any errata identified

Contributors and Schedule

- Committed Contributors
  - Ciena
  - Versa
  - Comcast
  - Cisco
- Schedule
  - Project Approval: This meeting
  - CFC #1:   Q4, 2023
  - CFC #2:   Q2, 2024
  - Letter Ballot: Q4, 2024

Secure Service Edge (SSE) Attributes

MEF

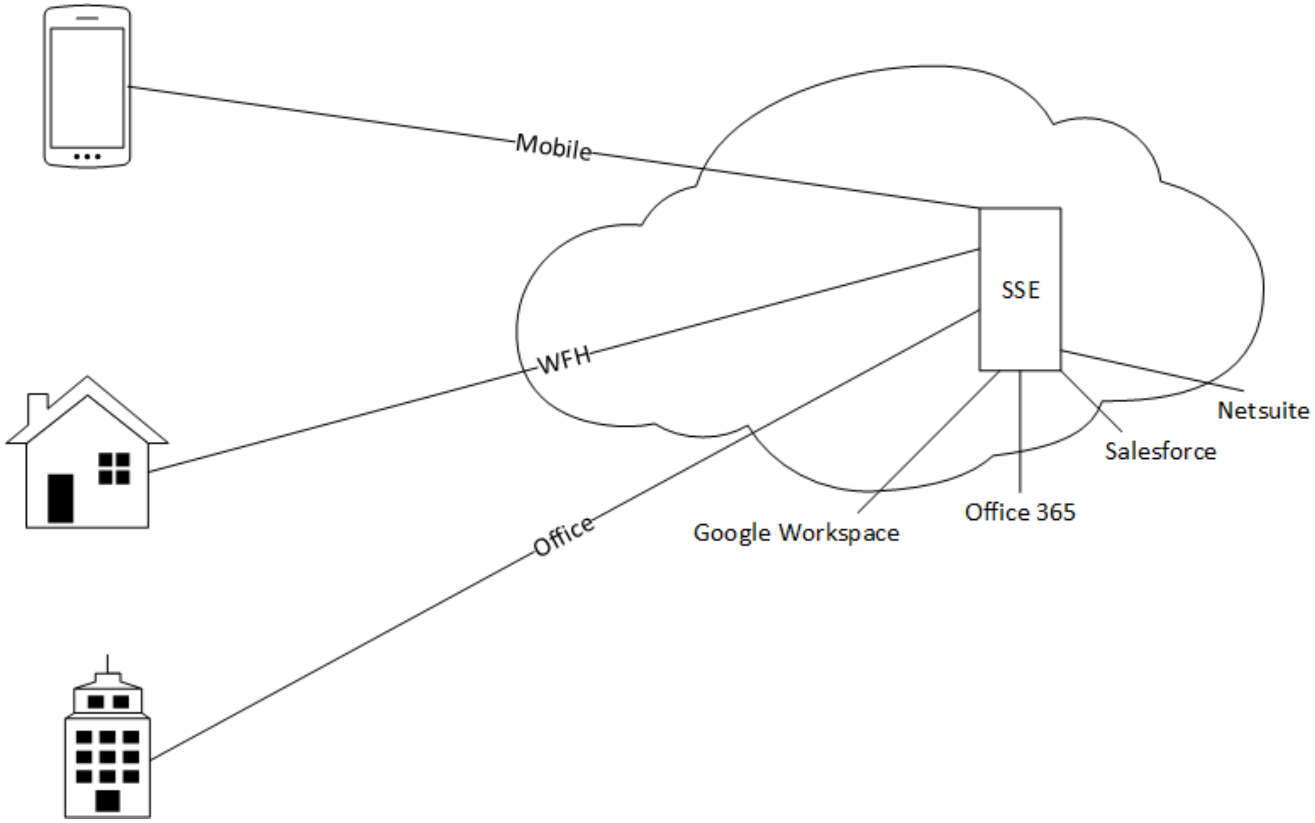
Spotlight on SASE
19 July 2023

SSE Building Blocks

- ZTNA
  - Limit access to specific applications
  - Everyone treated as bad Actor
- Access Control
  - Based on Policy
- Identity management for SaaS/IaaS
- Proxy
  - Forward
  - Reverse
  - OOB
- Action granularity
  - Store
  - Upload
  - Download
  - Permissions for others
  - Who it can be shared with

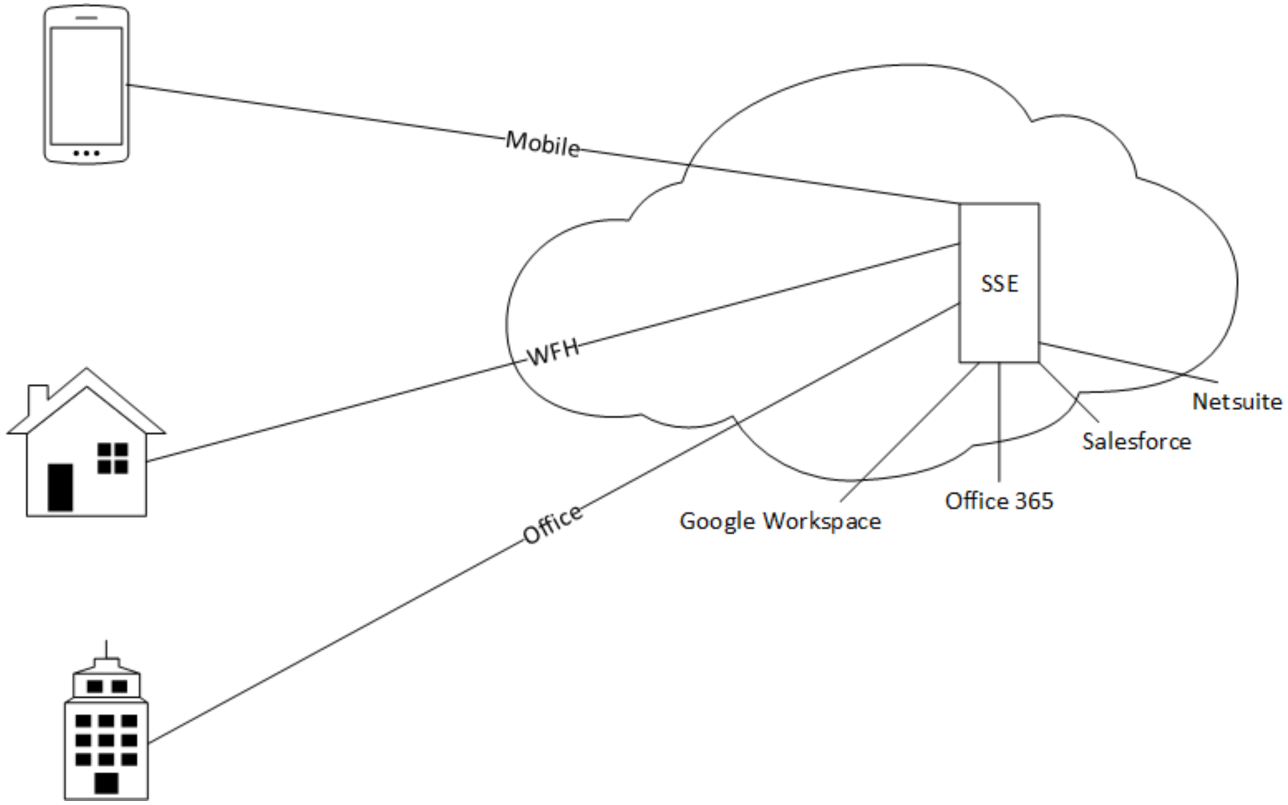
- IP Port and protocol filtering (W138)
- URL filtering (W138)
- Domain Name filtering (W138)
- Protected DNS (W138)
- OOB identification and mitigation
- IP Port and protocol filtering (W138)
- URL filtering (W138)
- Domain Name filtering (W138)
- Protected DNS (W138)
- Malware Detection and Removal (W138)
- SSL Encryption
- SSL Decryption
- SSL Bypass Decryption
- Learned patterns of user behavior
  - – AI
  - – Other methods
- Block requests outside of normal user behavior
- Quarantine web sites until they can be sanitized

Use Case 1 Secure Access



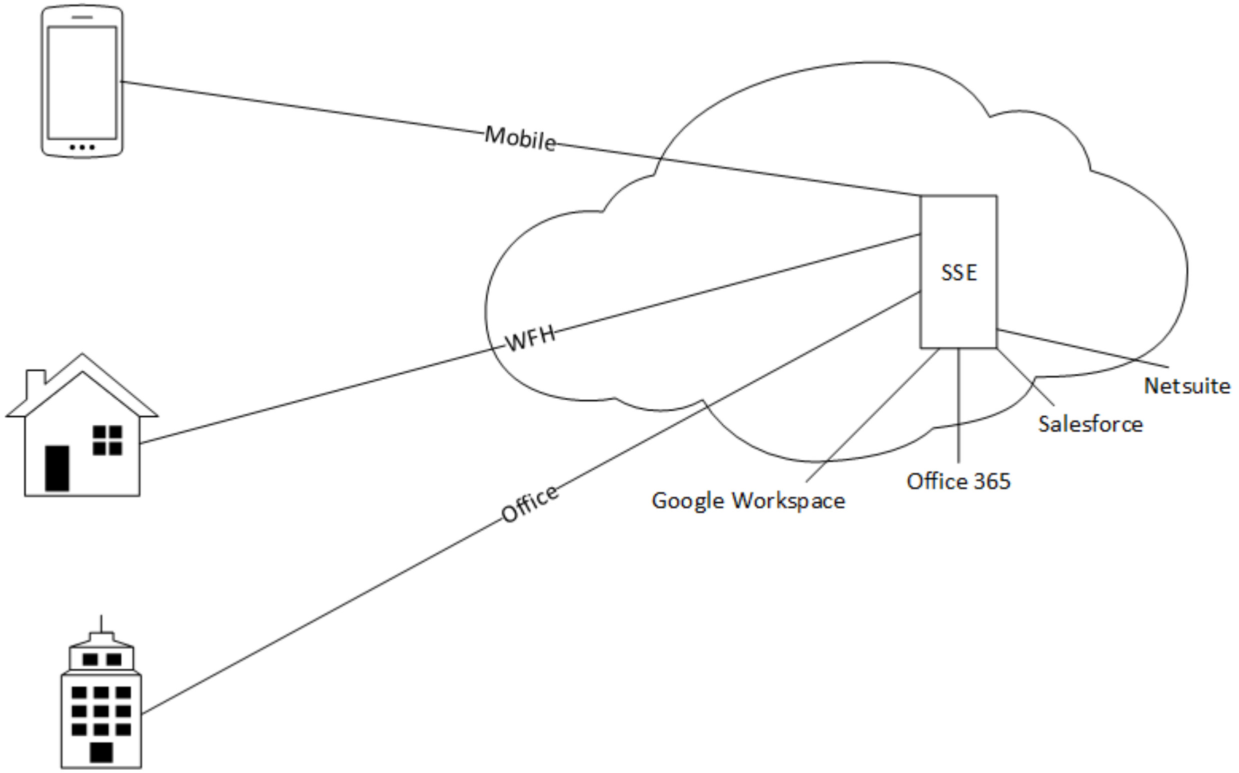
- ZTNA
  - Limit access to specific applications
  - Everyone treated as bad Actor
- Access Control
  - Based on Policy

Use Case 2 Data Security



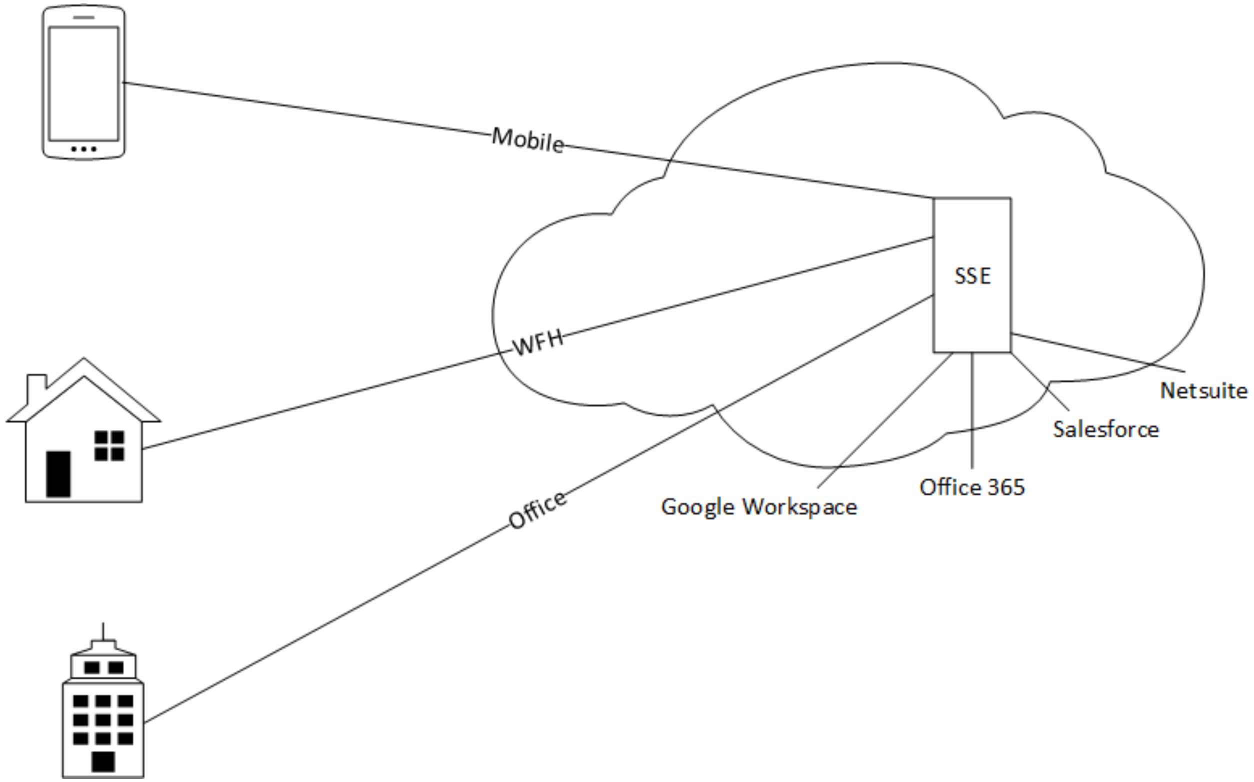
- Cloud Access Security Broker (CASB)
  - Identity management for SaaS/IaaS
  - Proxy
    - Forward/Reverse
    - OOB
  - Action granularity
    - Store
    - Upload
    - Download
    - Permissions for others
    - Who it can be shared with
- Data Loss Prevention (DLP)
  - Covered in W138
- SWG
  - Proxy
  - UNI termination
  - IP Port and protocol filtering (W138)
  - URL filtering (W138)
  - Domain Name filtering (W138)
  - Protected DNS (W138)

Use Case 3 Data Protection



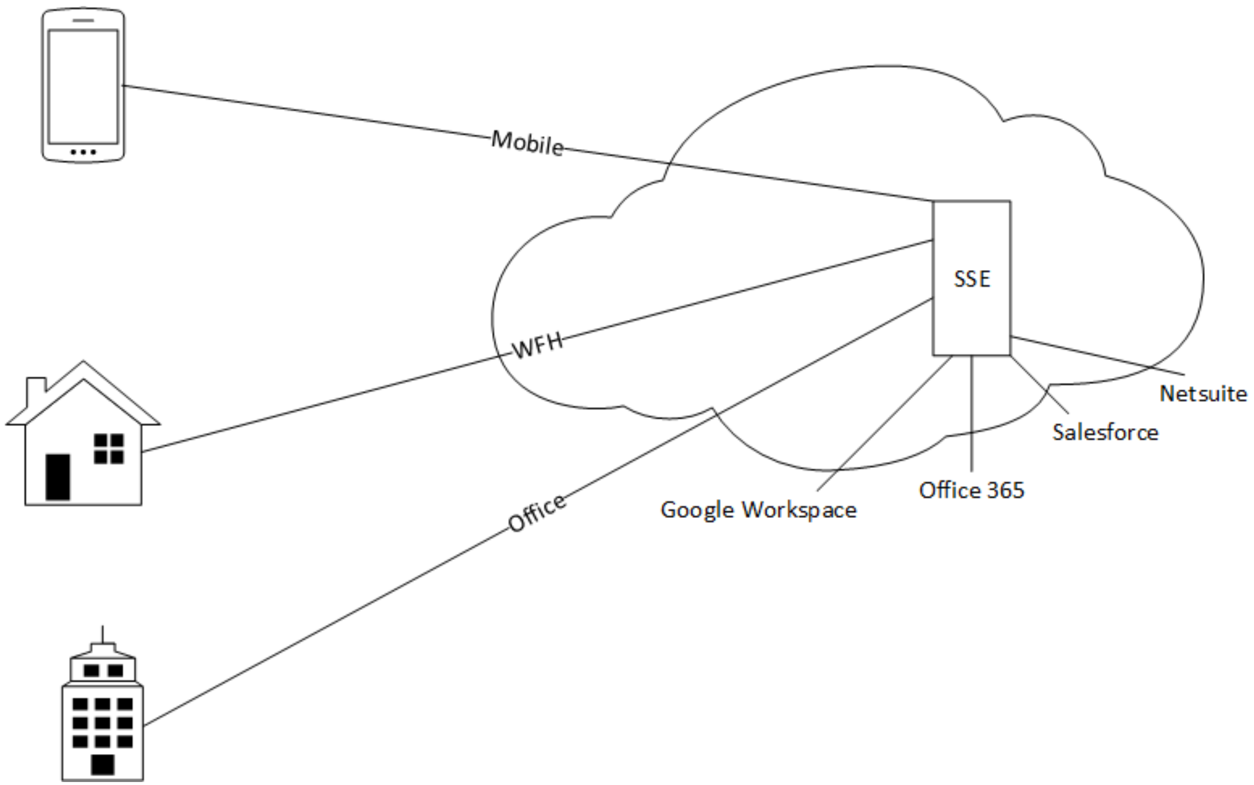
- Threat Identification and Mitigation
  - CASB
    - OOB identification and mitigation
  - FWaaS
    - IP Port and protocol filtering (W138)
    - URL filtering (W138)
    - Domain Name filtering (W138)
    - Protected DNS (W138)
    - Malware Detection and Removal (W138)
  - SWG
    - Proxy

Use Case 4 SSL Inspection



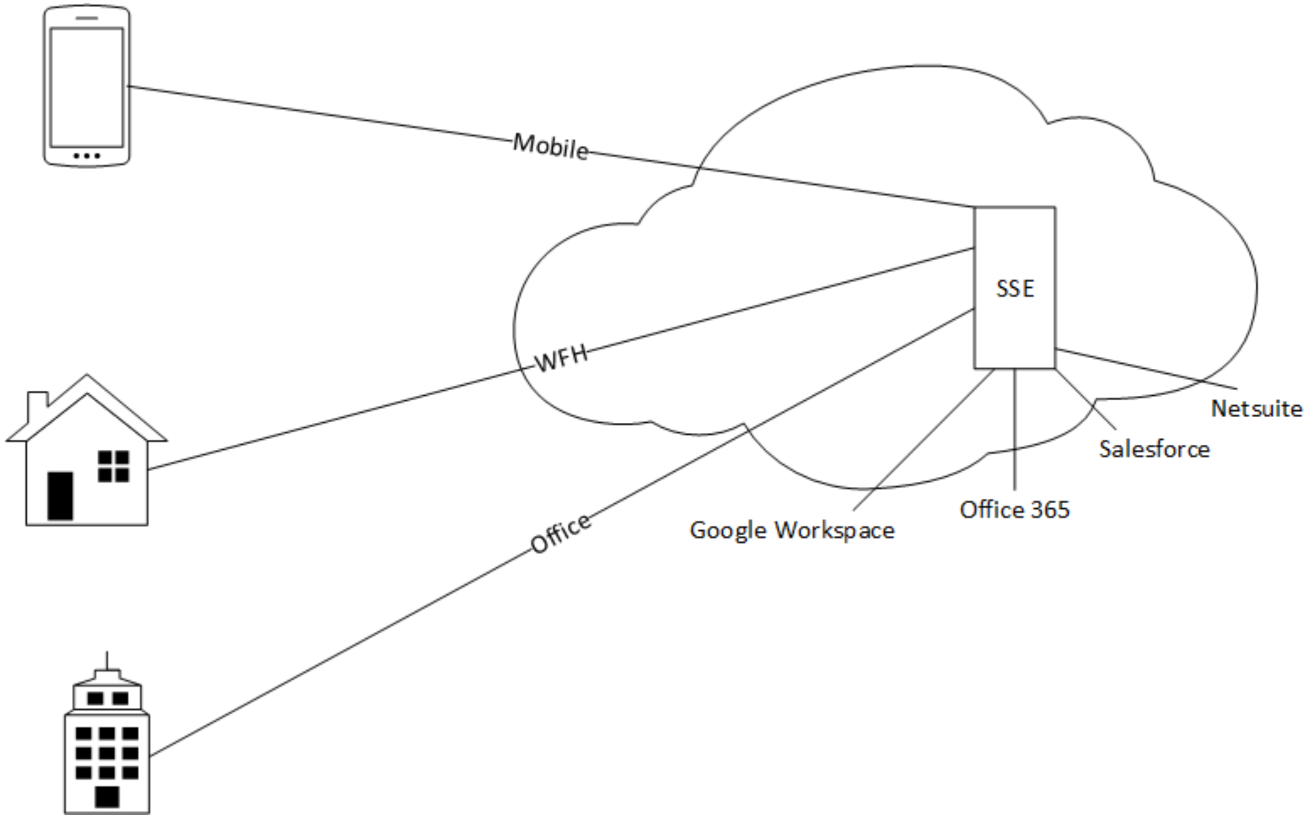
- SSL/TLS
  - Encryption
  - Decryption
  - Bypass Decryption
- Middlebox Security Function (W138)
- Cipher Suite support
  - Based on current cipher usage

Use Case 5 End User Behavior Analysis



- Learned patterns of user behavior
  - AI
  - Other methods
- Block requests outside of normal user behavior

Use Case 6 Remote Browser Isolation



- Quarantines web sites until they can be sanitized

Round Table Discussion

"WHY?"

Service Providers

- Why comply with these standards?
- Why get certified?
- Why mandate vendor compliance?
- Why participate in this work?

Vendors

- Why comply with these standards?
- Why get certified?
- Why participate in this work?

Break

SASE Certification

Vik Phatak
Chairman & CEO, CyberRatings.org

About Us

The benchmark for cybersecurity testing

- CyberRatings.org is non-profit member organization dedicated to providing confidence in cybersecurity products and services through our research and testing programs.

2500+ members from throughout the world include:

- Security Vendors
- Technology Companies
- Financial Services
- IT Services / MSPs
- International, Federal / State / Local Gov
- Healthcare
- Oil & Gas

Mission and Partnership

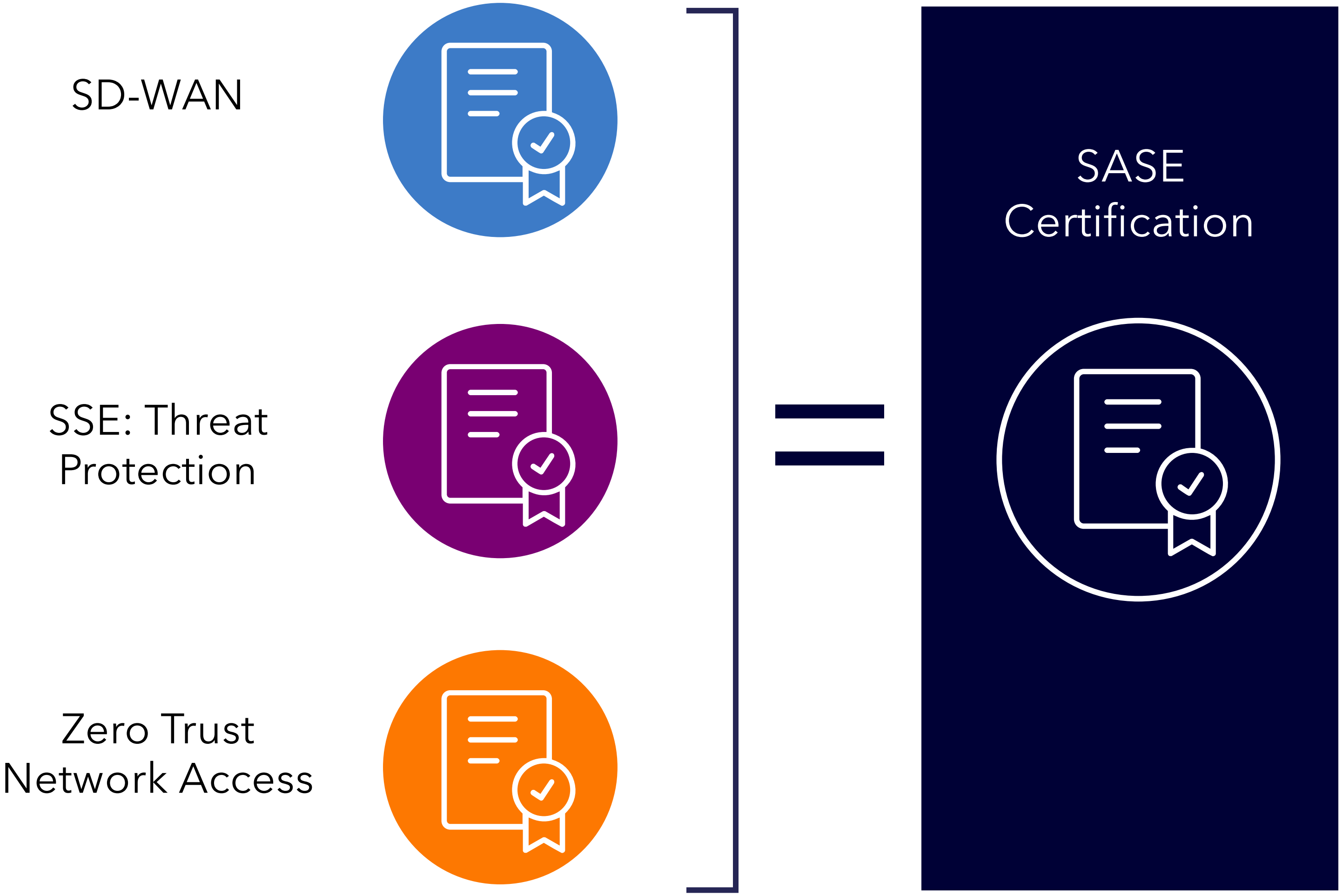
MEF's mission is to accelerate the worldwide adoption of assured services across automated networks.

CyberRatings.org is dedicated to providing confidence in cybersecurity products and services through our research and testing programs.

CyberRatings will perform Certification Services that comprise of either:

- Testing eligible devices, software, services, or other products that development by a technology provider / vendor MEF Member
- Certification of services that are provided by a MEF Service Provider Member

MEF SASE Certification Options



SD-WAN

SSE: Threat Protection

Zero Trust Network Access

SASE Certification

What is Driving SASE Adoption?

- Every network is unique; doesn’t scale
- Global shortage of cybersecurity professionals
- Security Service Edge (SSE) = cloud delivered security scales

- Pandemic changed work patterns; remote work is the norm
- Traditional VPNs don’t scale
- Zero Trust Network Access (ZTNA) = secure remote that scales

- SASE = SSE + ZTNA + SD-WAN

SASE is an approach that scales.

What is Driving SASE Adoption?

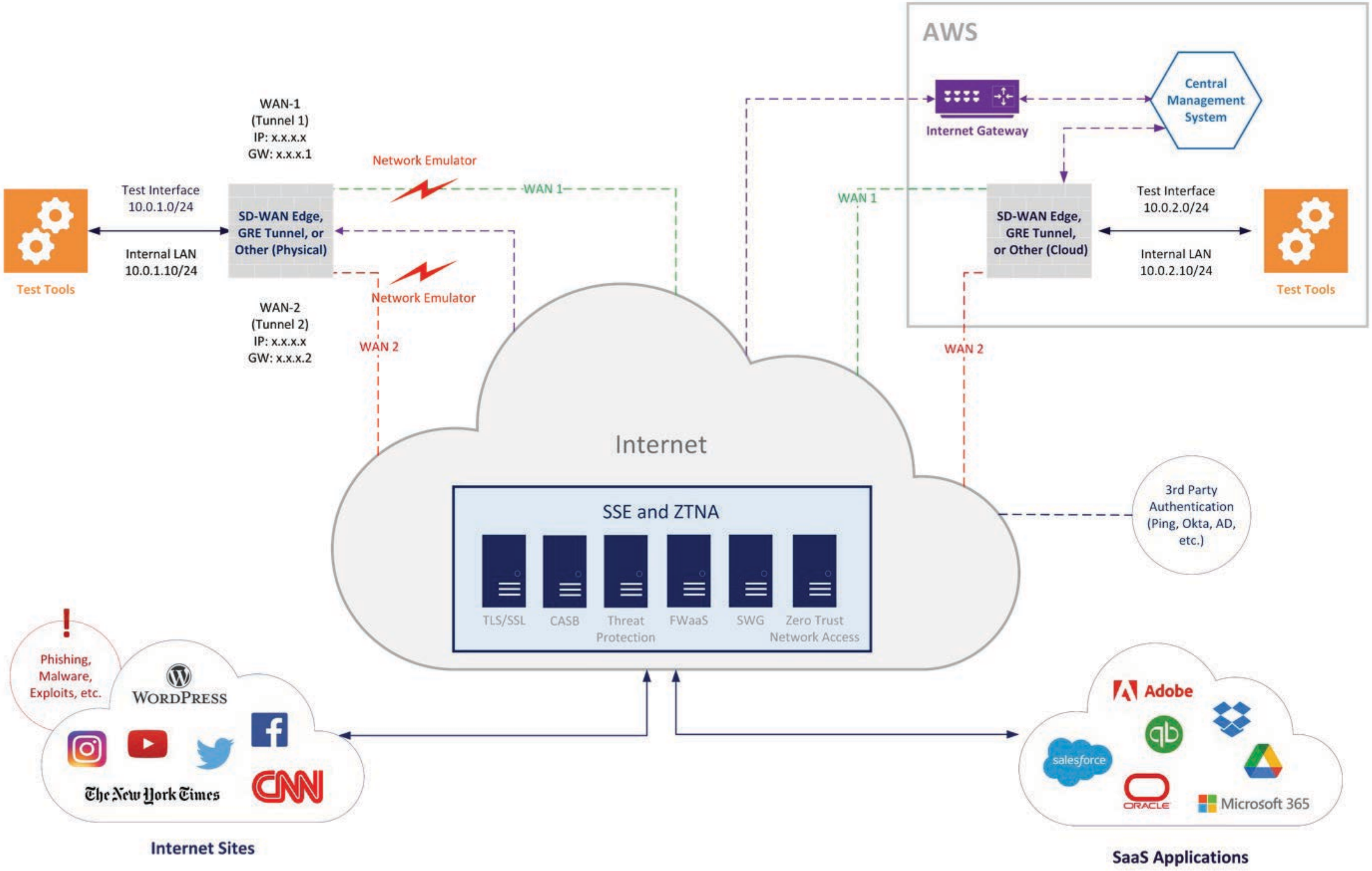
Secure Access Service Edge (SASE) market grew 55% year-over-year in Q1 2023 (Dell'Oro Group).

ZTNA is the fastest growing segment in network security and is forecast to grow 31% in 2023, up from less than 10% in 2021 (Gartner).

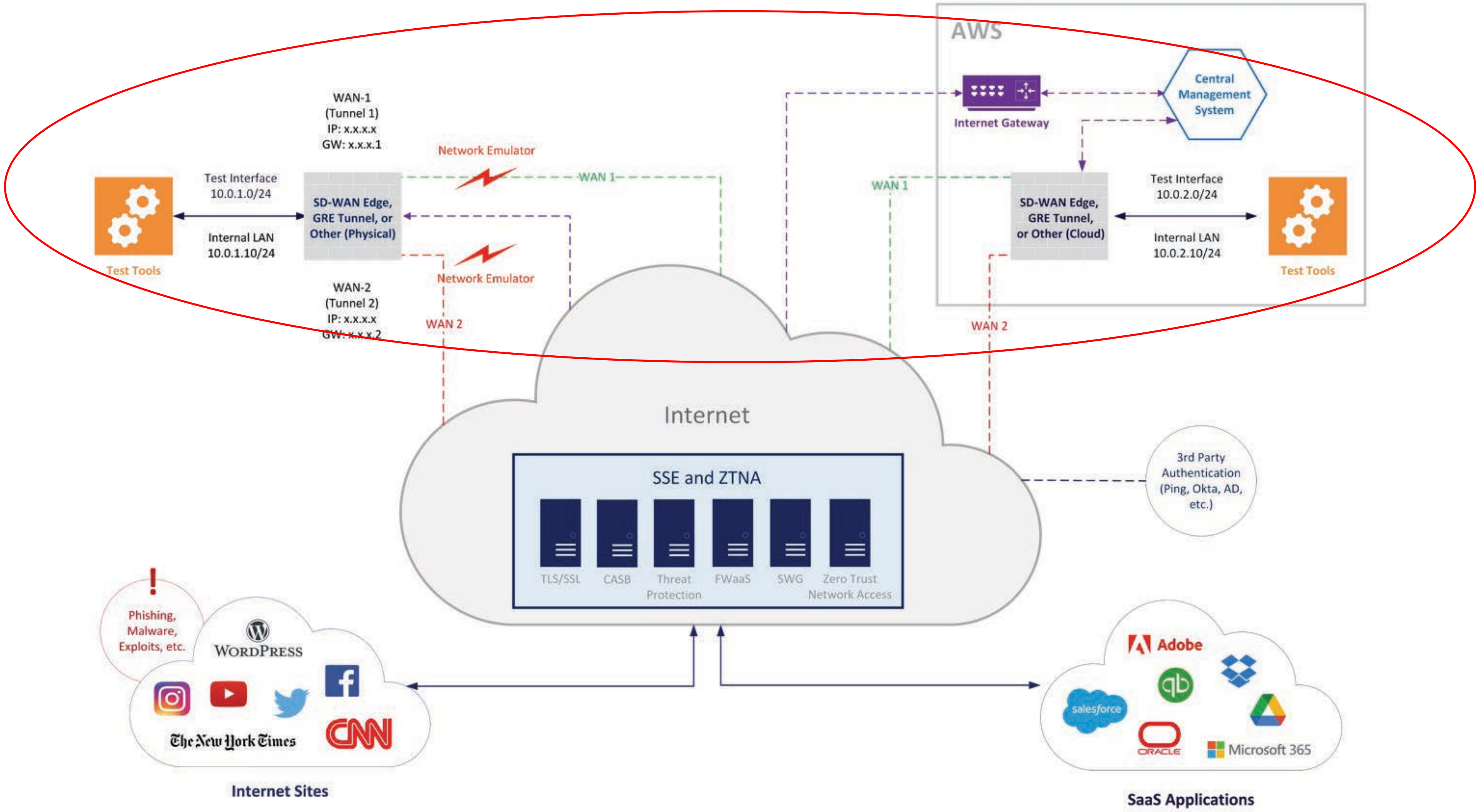
3.4 Million current shortage of cybersecurity workers. With SASE adoption, merging networking and security team silos will improve security and productivity. CIO – July 12, 2023

Built-in network support for ZTNA and SASE frameworks will help leaders deliver value faster. With the rapidly evolving threat landscape, this enhanced protection and simplified operations will help security teams advance initiatives securely. CIO – July 12, 2023

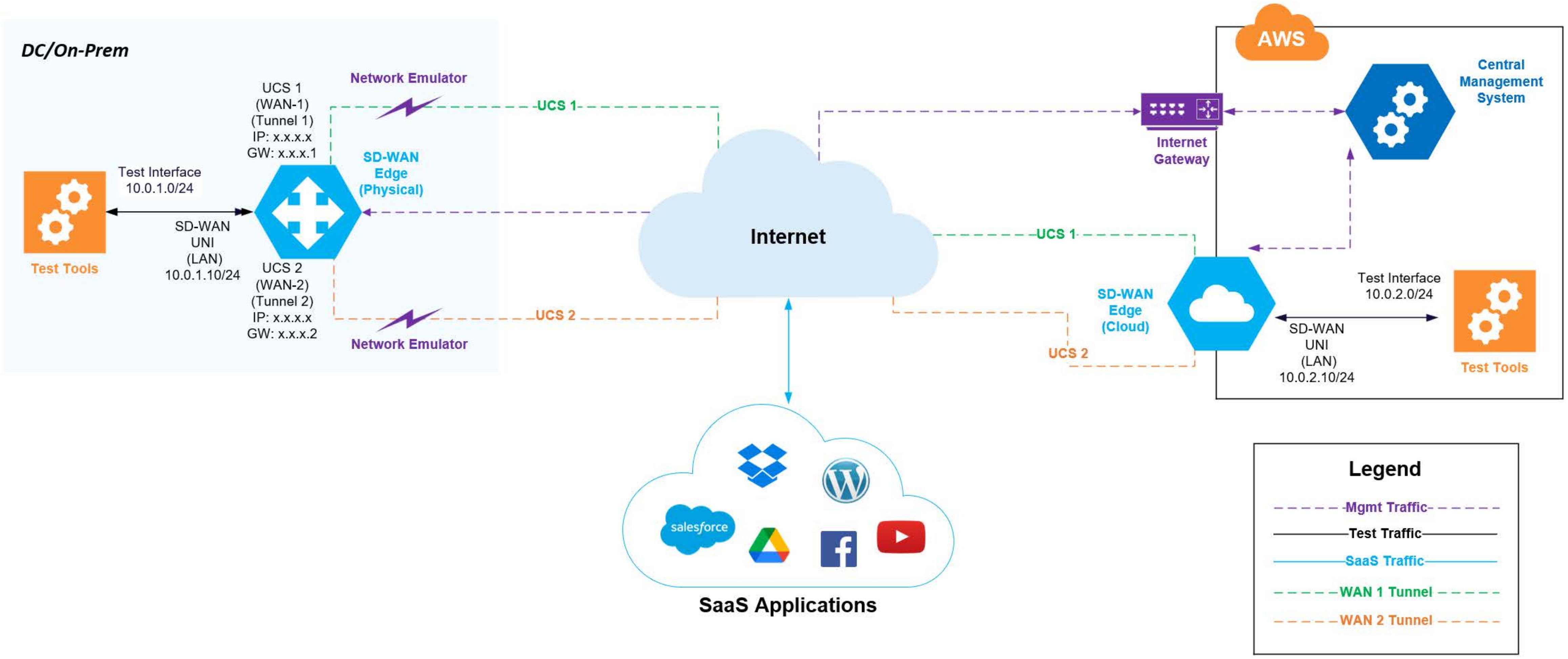
SASE Overview



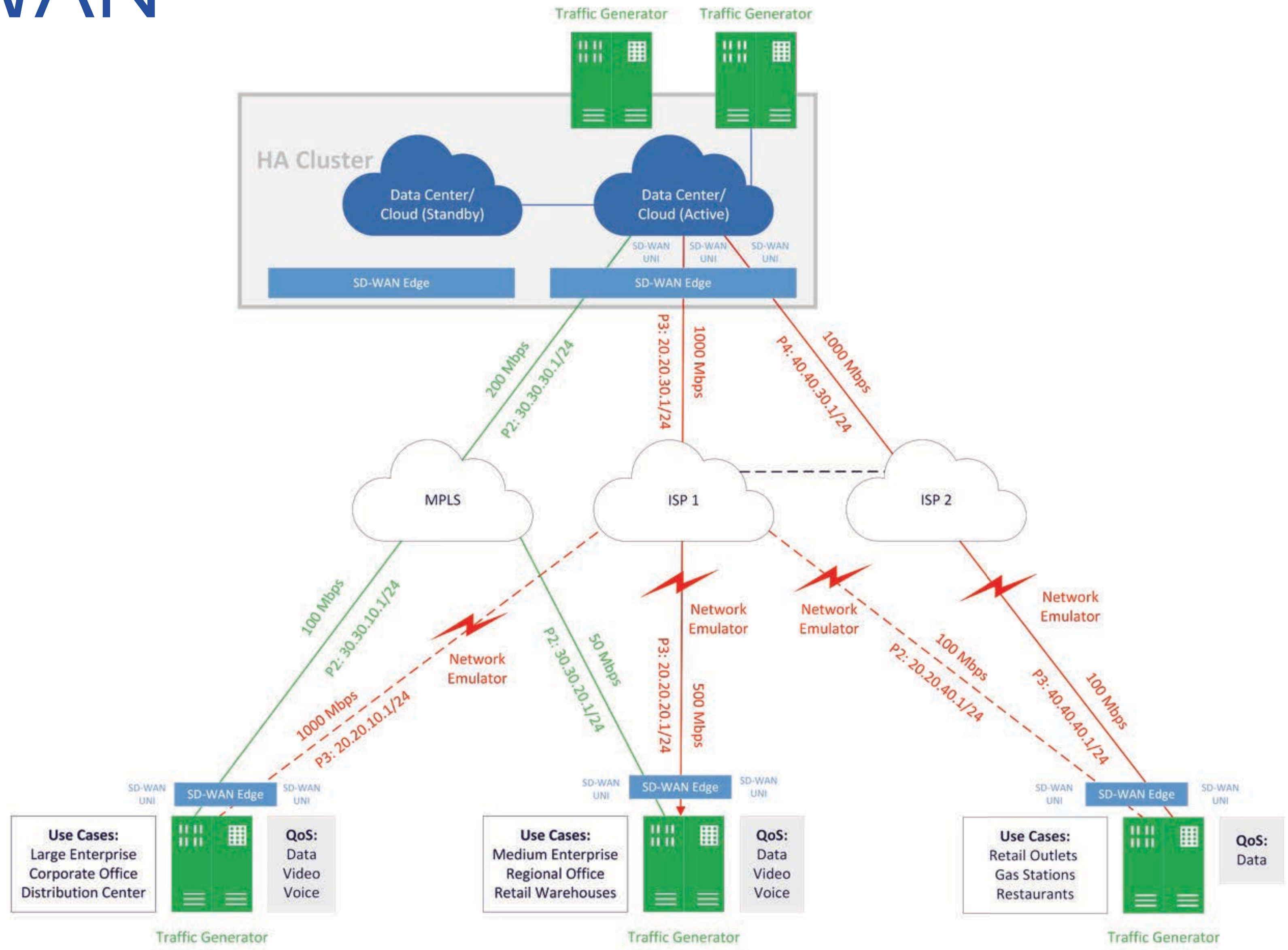
SD-WAN


AWS
Internet Gateway
Central Management System
WAN-1
(Tunnel 1)
IP: x.x.x.x
GW: x.x.x.1
Network Emulator
WAN 1
Test Interface
10.0.1.0/24
SD-WAN Edge, GRE Tunnel, or Other (Physical)
Internal LAN
10.0.1.10/24
Test Tools
Network Emulator
WAN-2
(Tunnel 2)
IP: x.x.x.x
GW: x.x.x.2
WAN 2
WAN 1
SD-WAN Edge, GRE Tunnel, or Other (Cloud)
Test Interface
10.0.2.0/24
Internal LAN
10.0.2.10/24
Test Tools
WAN 2
Internet
SSE and ZTNA
TLS/SSL
CASB
Threat Protection
FWaaS
SWG
Zero Trust Network Access
3rd Party Authentication (Ping, Okta, AD, etc.)
Phishing, Malware, Exploits, etc.
WordPress
The New York Times
CNN
Internet Sites
Adobe
salesforce
ORACLE
Microsoft 365
SaaS Applications

SD-WAN Overview



SD-WAN


Traffic Generator
Traffic Generator
HA Cluster
Data Center/ Cloud (Standby)
Data Center/ Cloud (Active)
SD-WAN UNI
SD-WAN UNI
SD-WAN UNI
SD-WAN Edge
SD-WAN Edge
200 Mbps
P2: 30.30.30.1/24
P3: 20.20.30.1/24
1000 Mbps
P4: 40.40.30.1/24
1000 Mbps
MPLS
ISP 1
ISP 2
100 Mbps
P2: 30.30.10.1/24
1000 Mbps
P3: 20.20.10.1/24
Network Emulator
P2: 30.30.20.1/24
50 Mbps
Network Emulator
P3: 20.20.20.1/24
500 Mbps
Network Emulator
100 Mbps
P2: 20.20.40.1/24
Network Emulator
P3: 40.40.40.1/24
100 Mbps
SD-WAN UNI
SD-WAN Edge
SD-WAN UNI
SD-WAN UNI
SD-WAN Edge
SD-WAN UNI
SD-WAN UNI
SD-WAN Edge
SD-WAN UNI
Use Cases: Large Enterprise Corporate Office Distribution Center
QoS: Data Video Voice
Traffic Generator
Use Cases: Medium Enterprise Regional Office Retail Warehouses
QoS: Data Video Voice
Traffic Generator
Use Cases: Retail Outlets Gas Stations Restaurants
QoS: Data
Traffic Generator

SD-WAN Certification

What constitutes an SD-WAN?

- Traditional routing and policy control features, including:
  - Basic application identification and policy controls
  - Stateful networking controls
  - Virtual private network (VPN)
- Prioritization of applications
- Remote configuration capabilities
- Predictable performance experience for users
- Highly resilient remote office connectivity

What will be tested?

- Routing
- Stateful Access Control
- Encryption
- Application Identification & Prioritization
- Management
- WAN Impairment
- Performance
- Stability & Reliability

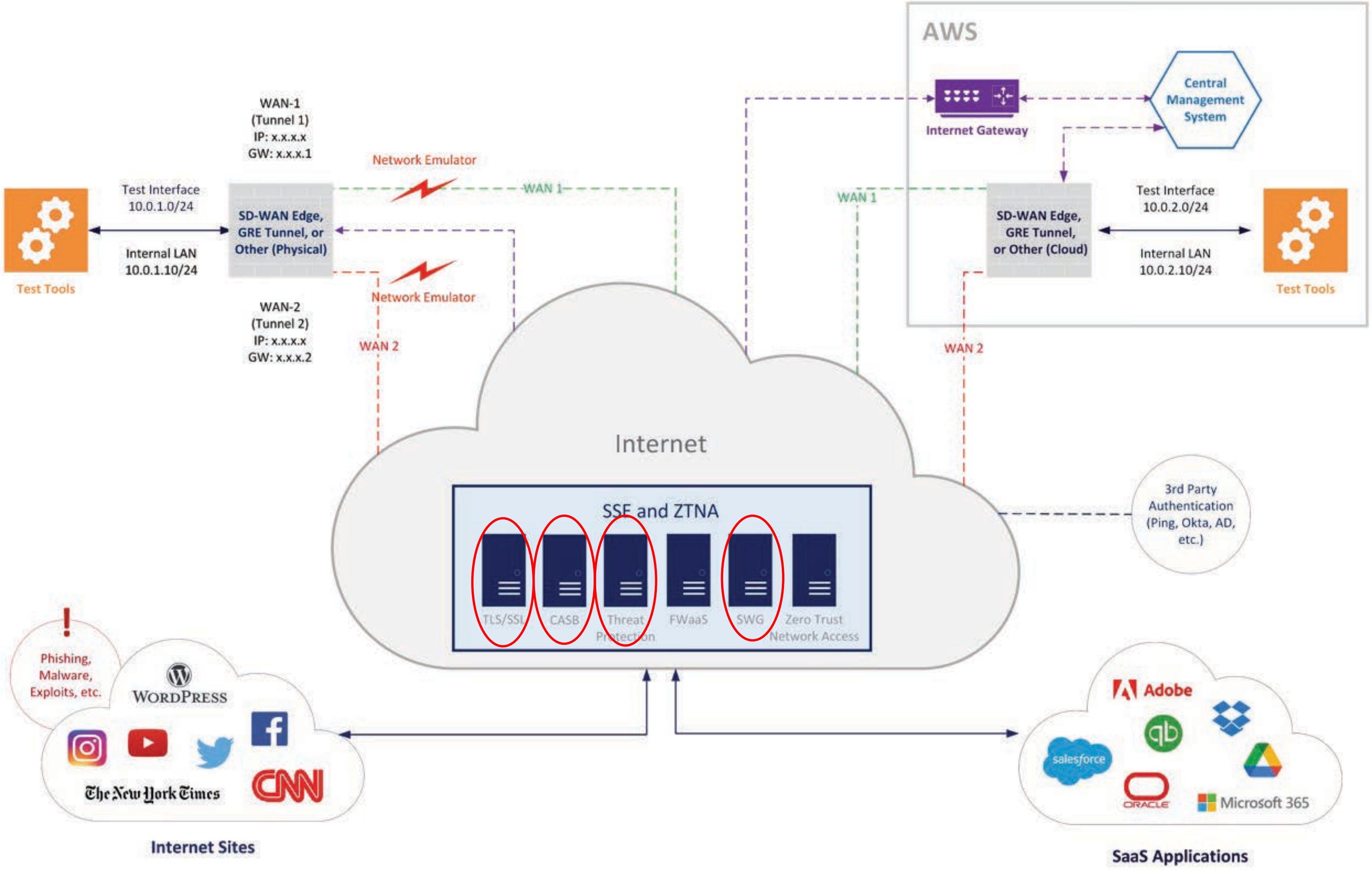
Report Card

Example SD-WAN Report Card

Vendor Name	Certification Date
Hardware Model	Software Version
Overall Score (AAA-D)	MEF Certification Pass or Fail
MEF Terminology Score	Routing and Access Control Score
SWVC Performance Score	UCS Impairment Score
SWVC Stability and Reliability Score	

- After the completion of each testing session, the test house issues a report card based on the results of the testing.
- The scores from each area are calculated based on 800 points being associated with each area, the penalties associated with different testing results and then a score per area is determined.
- The area scores are averaged, determining the Overall Score.

SSE - Threat Protection



MEF

SSE Threat Protection Certification

- **Authentication and Identity**
  - SAML Authentication via integration with Identity Providers (IdP)
- **SSL / TLS Functionality**
  - Supported Cipher Suites
  - Decryption Validation and Bypass Exceptions
- **HTTP / HTTPS Performance**
  - Top 4 cipher suites (98%+ of web traffic)
- **Cloud Access Security Broker**
  - Cloud Access
  - Cloud Application Control
- **Anti-Malware (AV), Intrusion Prevention (IPS), Malware Sandbox, Secure Web Gateway (SWG):**
  - Exploit Protection
  - Malware Protection
  - Resistance to Evasions
  - Zero Day and Custom Malware Protection

- **Live, real-time testing** of malware, exploits, URLs
- **4,000+ exploits in library** (an exploit is an attack that takes advantage of a vulnerability in a protocol, product, operating system, or application)
- **12,000+ evasions** (evasions disguise and modify attacks to avoid detection by security products)
- **100,000+ simultaneous VMs** for emulating large environments
- **1,000,000+ fresh malware samples** per month
- **Multiple terabits** of performance

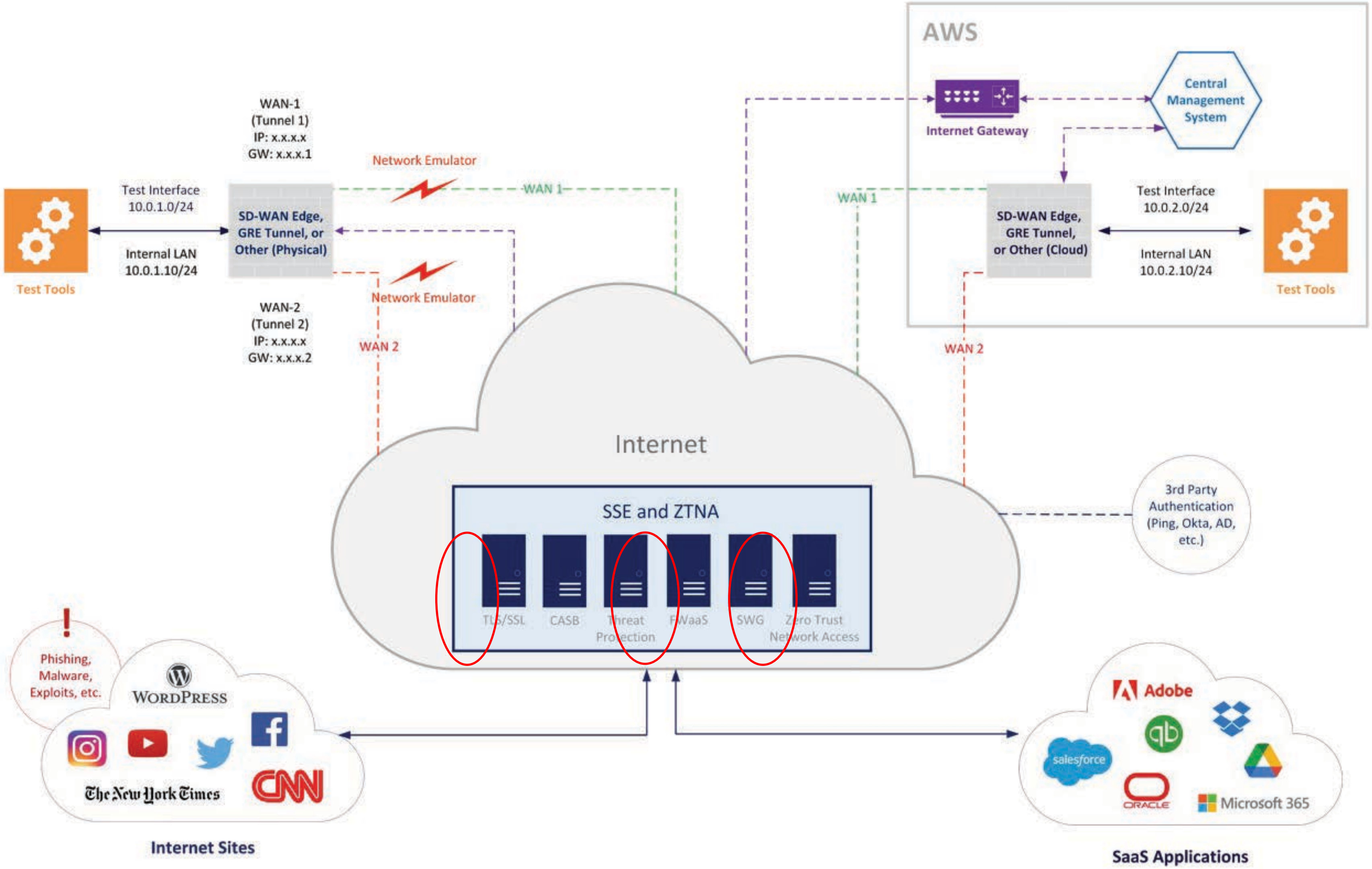
Report Card

Example SSE Report Card

Vendor Name	Certification Date
Hardware Model	Software Version
Overall Score (AAA-D)	MEF Certification Pass or Fail
MEF Terminology Score	Routing Functionality Score
SSL/TLS Support Score	Management Capabilities Score
Reporting Capabilities Score	Cloud Access/Application Control Score
Threat Prevention Score	Evasions Score

- After the completion of each testing session, the test house issues a report card based on the results of the testing.
- The scores from each area are calculated based on 800 points being associated with each area, the penalties associated with different testing results and then a score per area is determined.
- The area scores are averaged, determining the Overall Score.

Zero Trust Network Access



ZTNA Certification

- **Authentication and Identity**
  - SAML Authentication via integration with Identity Providers (IdP)
- **SSL / TLS Functionality**
  - Supported Cipher Suites
  - Decryption Validation and Bypass Exceptions
- **HTTP / HTTPS Performance**
  - Top 4 cipher suites (98%+ of web traffic)
- **Zero Trust Network Access (ZTNA) and Firewall**
  - Access Control
  - Application Control
  - Policy Enforcement
  - Network Segmentation & Routing

Example ZTNA Report Card

Vendor Name	Certification Date
Hardware Model	Software Version
Overall Score (AAA-D)	MEF Certification Pass or Fail
MEF Terminology Score	Policy Enforcement Score
Management Capabilities Score	Reporting Capabilities Score
Cloud Access/Application Control Score	

Certification Phases

Phase 1

Beta Program:

- Test and Certify Vendor technologies represented on the Technical Advisory Board
- Service Providers represented on the Board of Directors will inherit the Certifications of those Vendors who have been tested and certified.

Generally Available (GA):

- Test and Certify Vendor technologies represented by MEF members at large
- Service Providers who are MEF members at large will inherit Certifications of those Vendors who have been tested and certified.

Phase 2

Beta Program:

- Everything
- Certification of Service Providers (Board of Directors) based on their value-add criteria TBD
  - Considering IT service management (ITSM) & Information Technology

Generally Available (GA):

- Test and Certify Service Providers who are MEF members at large.

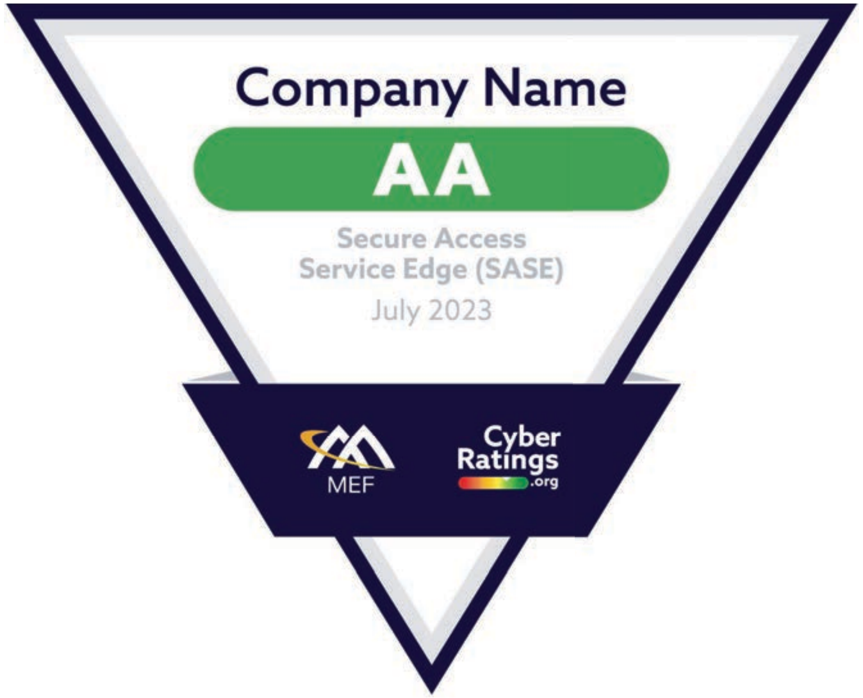
Pricing Model with Bundling

	SD-WAN	SSE or ZTNA Standalone	SSE/ZTNA Bundle
Vendor	$15,000 per product series	$25,000 per product series	$40,000 per product series
Service Provider	$30,000	$30,000	$40,000

Notes/Inclusions:

1. SASE = SD/WAN + SSE + Zero Trust Network Access
2. Testing is vendor-only, certified product and version for SPs is verified for initial certification
3. Member can certify one, two or all of the SASE certifications and will be recognized as SASE certified if all three are achieved
4. Yearly ongoing subscription required to maintain a valid certification and badge
5. Ability to improve rating during subscription period
6. Consideration for special price migration path for recently certified members

SASE Badge Example



Rating is calculated on a scale from 0 to 800, based on Security Effectiveness, Performance, and Functionality

Rating	Min	Max
AAA	775	800
AA	720	774
A	660	719
BBB	590	659
BB	540	589
B	480	539
CCC	420	479
CC	360	419
C	300	359
D	0	299

Thank You!

Vikram Phatak, CEO

vik@cyberratings.org

SASE Marketing

Kevin Vachon
COO, MEF

MEF

Spotlight on SASE
19 July 2023

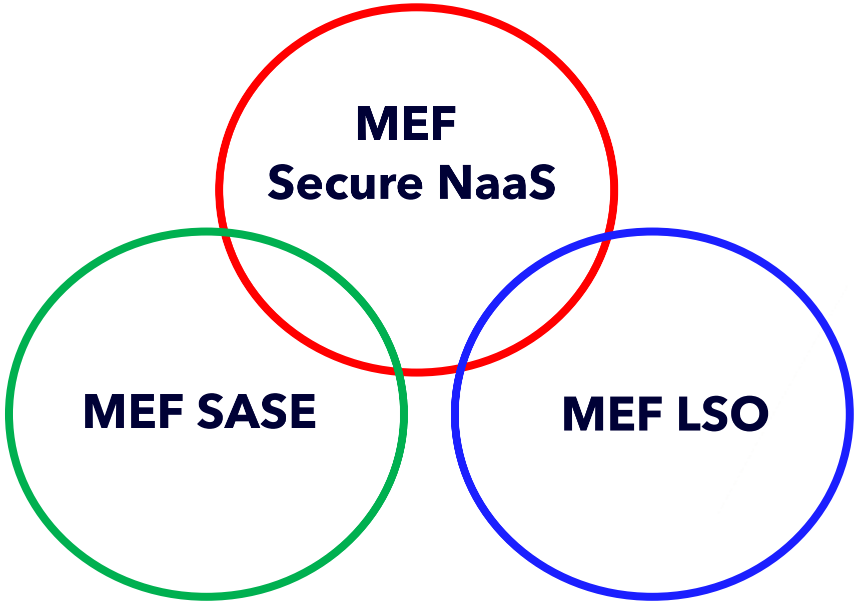
Marketing

SASE Certification Marketing Strategy

- *Initial* – Lead with SASE certification - educate & create demand for vendor and service provider certifications
- *Next* - Incubate enterprise awareness of SASE certification availability and generate demand for SP certifications
- *Ongoing* – Create enterprise demand for MEF SASE certification and standards
    - By raising awareness level across a broad but well-defined set of industry stakeholders/influencers – enterprises, consultants, press, analysts, SPs, vendors etc.

SASE and the Overall MEF Marketing Plan

- SASE is one of 3 “Product” pillars for MEF marketing in Fiscal 24 (July 23- June 24)
- Secure NaaS will pull through both SASE and LSO
- SASE and LSO are also marketed as standalone topics



Preliminary Deliverables – SASE Certification

Assets

- Messaging
- MEF.net info pages & registries
- Datasheets & contracts
- Standard presentations
- FAQ document
- Videos
- Press releases
- Published articles and blogs
- Certification marketing kit

Activities & Milestones

- MEF-CR relationship PR – July 26
- Detailed marketing plan – Aug 30
- Asset development (Current- Sept 15)
- Beta announcement – ~ Sept 6
- Inclusion in GNE program - Oct 3
- GA launch (Jan 24)
  - PR, press & analyst pre-briefings
  - Emails, social media posts and ads
  - Certified Member co-marketing for amplification
  - Other

MEF

SASE Industry Perspectives

Sunil Khandekar

(**Moderator**) Tech Executive, Advisor, Former Founder & CEO at Nuage Networks

Ari Banerjee

SVP, Netcracker Technology

Neil Danilowicz

Principal Architect, Versa Networks

Daniele Mancuso

CPM, Sparkle

Franck Morales

VP, Evolution Platform, Orange Business

Tom Schnarr

PM, Telecom, Media, Technology, ServiceNow

Mirko Voltolini

VP, Innovation, Colt Technology

MEF

Spotlight on SASE
19 July 2023

Closing Remarks

Kevin Vachon
MEF COO

MEF

Spotlight on SASE
19 July 2023

Closing Remarks

- Engage in the SASE standardization
  - Participate on weekly calls
  - Participate in review for Call for Comments (CfCB) process
  - Vote on standards
- Propose innovative new work projects
- Help us educate
- Get SASE certified (when publicly available)

Create impact!