LF NETWORKING

LFN Developer & Testing Forum

Cloud Native SASE and EMCO

Srinivasa Addepalli, Intel
Srinivasa Addepalli | LinkedIn

Anti-Trust Policy Notice

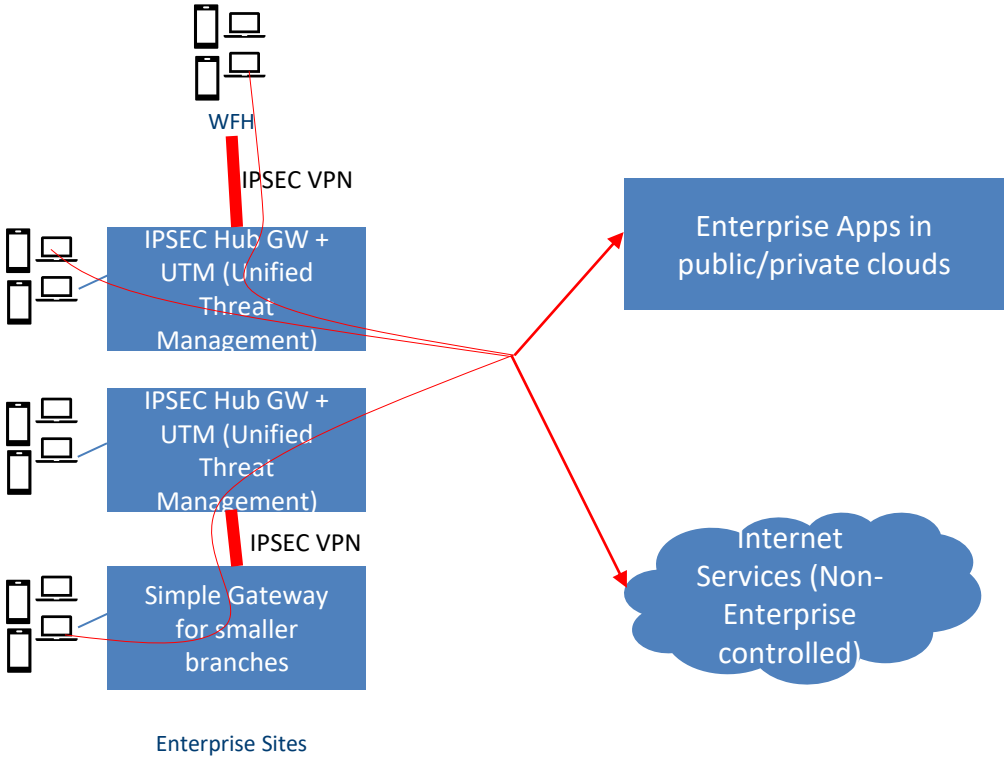
- Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrustpolicy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Outline

- SASE – Introduction
- Current SASE Architecture
- 2nd Generation Cloud Native SASE Architecture
- 3rd Generation Cloud Native SASE with Service Mesh
- Role of Nodus, EMCO and Service Mesh
- Request for SASE framework features in EMCO
- Q&A

Protecting client device assets and thereby data assets from lateral attacks – old way



Client and Data assets protected by UTM

UTM consists multiple threat security functions - Firewall, IDS/IPS, Anti-Malware, URL filtering, IP/Domain filtering, & Observability function.

IPSEC Hubs are used for tunneling traffic through UTMs

Security is realized by Enterprises by UTMs in main Enterprise sites

All the traffic is passed through UTMs for security scanning and enforcement

Case for SASE

User anywhere (Geo Distributed Workforce)
WFH, Remote User, Branch Offices ; Significant growth of traffic from WFH/Remote users

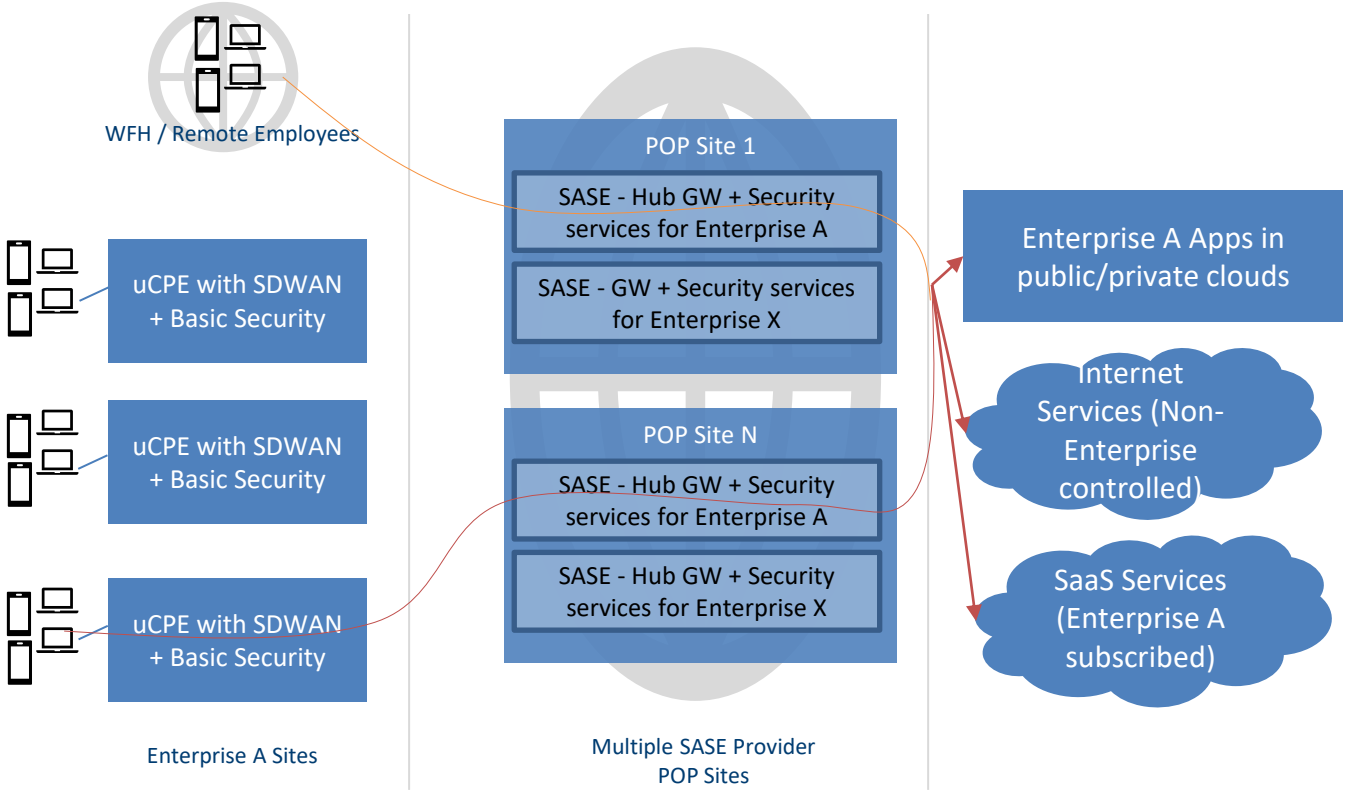
Service Anywhere (Geo Distributed Services)
Private DC, Public Cloud, SaaS, Edge

All traffic is encrypted
95% of web traffic is encrypted (TLS)

Challenges with old ways
Routing traffic via Enterprise DC for security scanning is costly, degrades user experience; skillset challenges with increasing complexity of cybersecurity; Higher maintenance of UTM & Gateways

Need for distributed security for distributed workforce & for anywhere services
Hence SASE (Secure Access Service Edge)

Protecting assets – SASE Way



Provide low-latency access to users, devices and cloud services anywhere, Enterprises are provided with SASE offerings with a worldwide fabric of points of presence (POPs) and peering relationships.

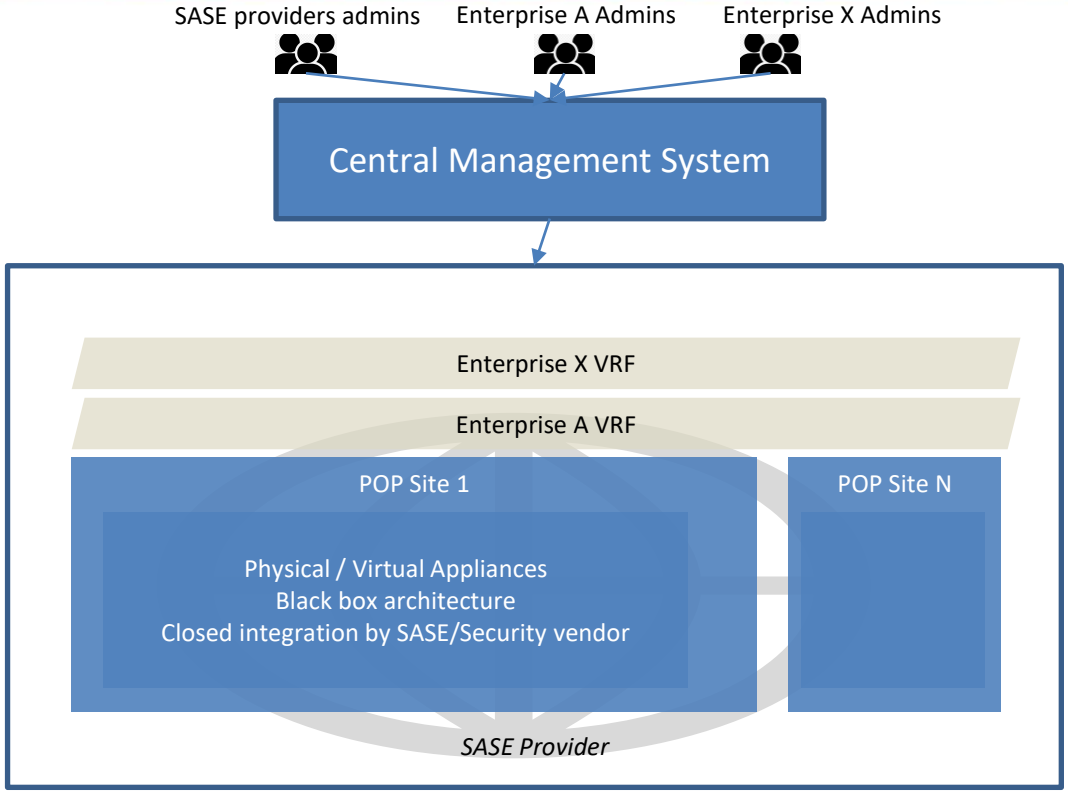
Managed / Co-managed service reduces the skillset challenges

Addresses digital businesses where users, devices, applications and services are located outside of Enterprise premises.

Gartner findings

- By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor up from less than 5% in 2019.
- By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018.
- *By 2025, at least one of the leading IaaS providers will offer a competitive suite of SASE capabilities.*
- *TLS Inspection is MUST for SASE*

SASE Architecture – Current Generation



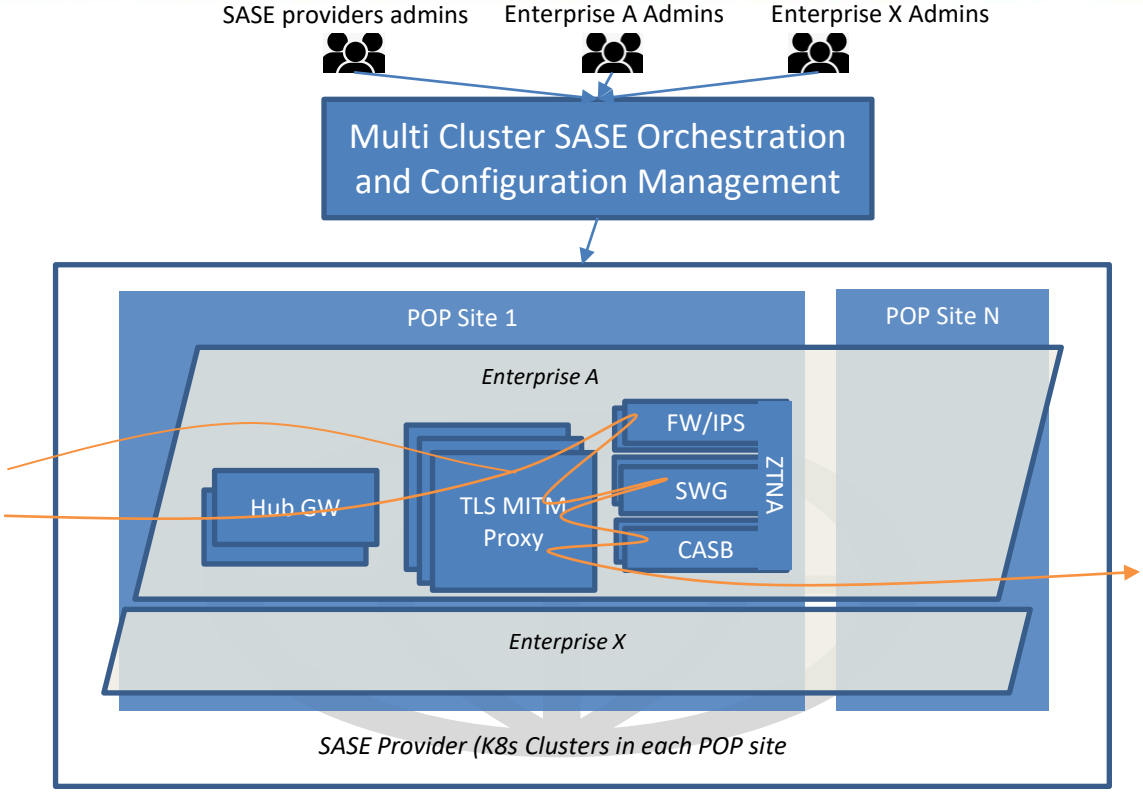
- Black box architecture
- Same SASE functions for every Enterprise
- Virtual/Physical Appliance based

Few challenges

- Scale Out & Load sharing
- High availability & Upgrades
- Performance isolation among Enterprises
- Security (private keys, secrets, passwords) isolation among Enterprises
- No choice of selection of security functions by Enterprises

Scaling & isolations are normally taken care in proprietary way

SASE Architecture – 2nd Generation
Cloud Native SASE 2.0



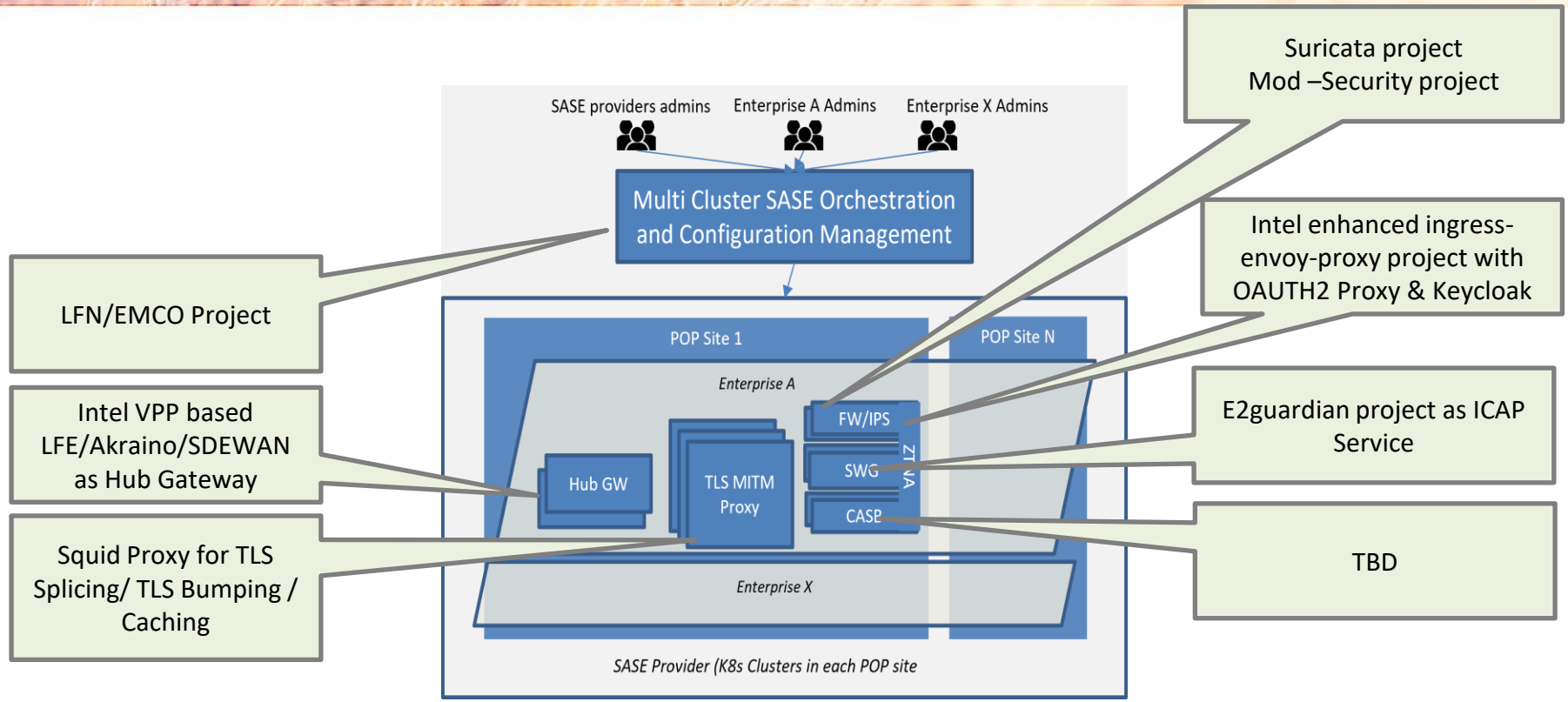
- K8s (Cloud Native) Architecture
- Container based
- On-demand instantiation across PoPs based on tenant requirements

Addressing Challenges with Open Arch

- Scale Out & Load sharing (Use K8s and its ecosystem such as MetalLB, IPVS)
- High availability & Upgrades (Use K8s & its ecosystem such as Global DNS Server automation & Rolling upgrades)
- Performance isolation among Enterprises (Separate containers for each tenant and let K8s take care of fair sharing)
- Security (private keys, secrets, passwords) isolation among Enterprises (Use K8s separate containers with DHSM – Any exploitation only exfiltrates that specific container information)
- No choice of selection of security functions by Enterprises (Different vendor security functions as containers can be chosen for each Enterprise)

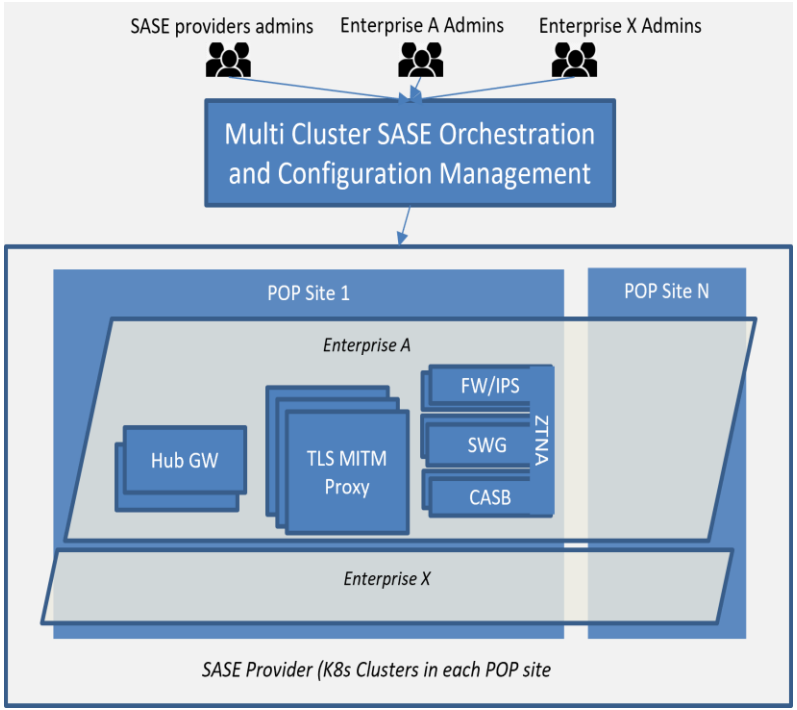
SASE Architecture – 2nd Generation (Opensource Software Mapping)

LFN NETWORKING
LFN Developer & Testing Forum



LFE/Akraino/Nodus & SDEWAN projects – Intends to automate configuration of Squid proxy with ICAP based SFC & showcase E2E solution

SASE Architecture – 2nd Generation Challenges & Opportunities



Opportunity for higher efficient system architecture

- *Single pass architecture - Avoid too many TCP/IP traversals resulting from ICAP based architecture.*

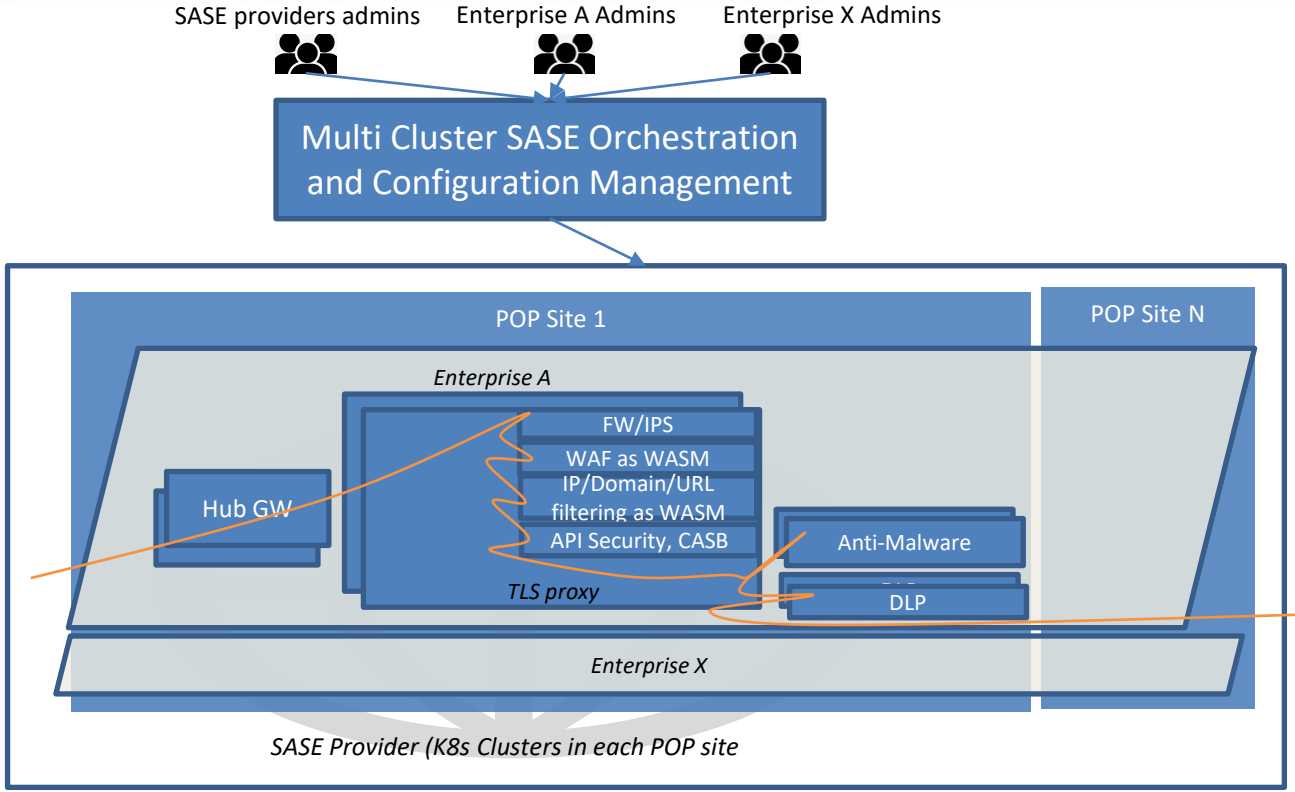
Opportunity for Multi vendor SASE even with single pass

- *Such as WASM based security functions*

Opportunities to avoid multiple software blocks

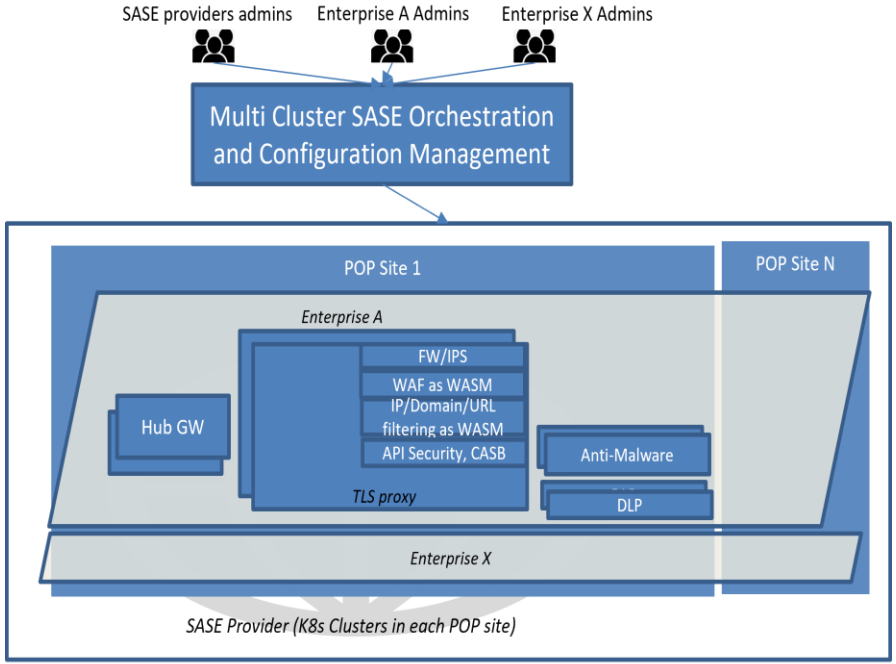
- *Combine ZTNA with Proxy*

SASE Architecture – 3rd Generation
Cloud Native SASE 3.0



- As many functions as possible as WASM Modules
- Multi vendor WASM based security functions
- SWG divided into two – IP/Domain/URL filtering as WASM and Anti-Malware as ICAP service.
- Complex security functions can continue to be ICAP services
- If DLP-as-a-Service is used (such as Google Cloud DLP), then DLP can be WASM module too.

SASE Architecture – 3rd Generation
Service Mesh project work items



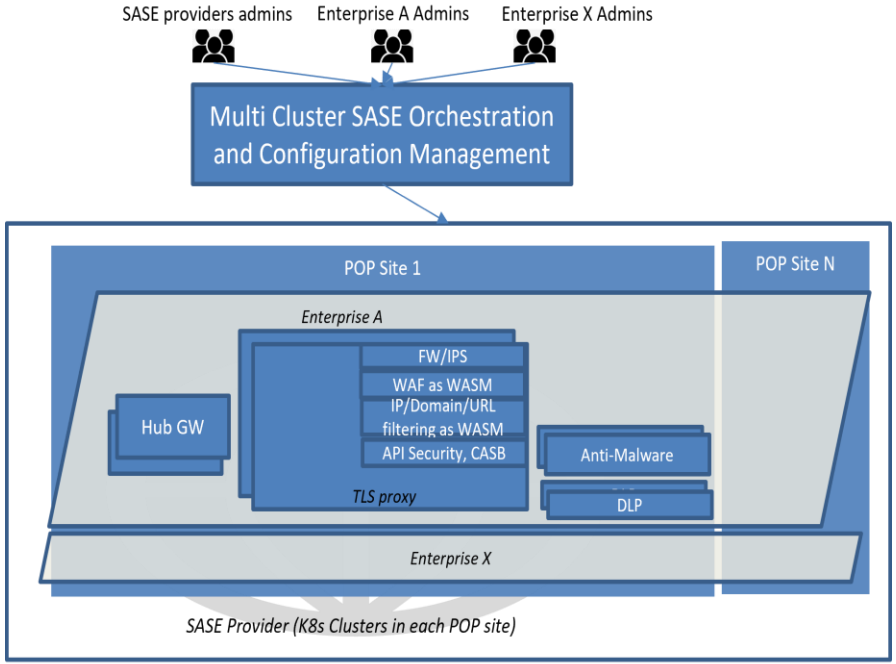
Envoy as Proxy & Cache

Intel Service Mesh initiative added TLS Splicing/Bumping to Envoy; Mod-Security WASM Module

WIP:

- Integration of Caching technology
- ICAP support
- SFC with tenant defined SFs across WASM plugins & ICAP plugins.
- K8s native configuration (CR based)
- Google Cloud DLP as WASM Plugin
- ClamAV based Anti-Malware as ICAP service
- IP/Domain/URL filtering with Google Webrisk as WASM module

SASE Architecture – 3rd Generation
EMCO project work items



EMCO as Multi Cluster SASE Orchestration & configuration management

Request for following features in EMCO (Core & Ecosystem)

- A way to onboard WASM modules.
- A way to define WASM Modules and ICAP filters to be used for a given tenant & POP location.
- A way to deploy WASM modules on running Envoy
- A way to configure Envoy proxy using K8s CRs.
- A way to automate the configuration of WASM Plugin and ICAP plugins.
- Automate configuration of ISTIO, OAUTH2-proxy and keyCloak for ZTNA authentication functionality.

Conclusion

- SASE market is growing
- We believe productivity improvements with Cloud native SASE – Scale; upgrade; better perf/security isolation
- Leveraging service mesh also improves performance and provides multi vendor SASE functionality.
- Intel is contributing features in open-source projects to realize cloud native SASE
- Please contact @Sundar Nadathur and @Srinivasa Addepalli for more information

LF NETWORKING

LFN Developer & Testing Forum