Unleash the Full Power of SASE-on-SIM

Versa SASE For Packet Core Network

White Paper

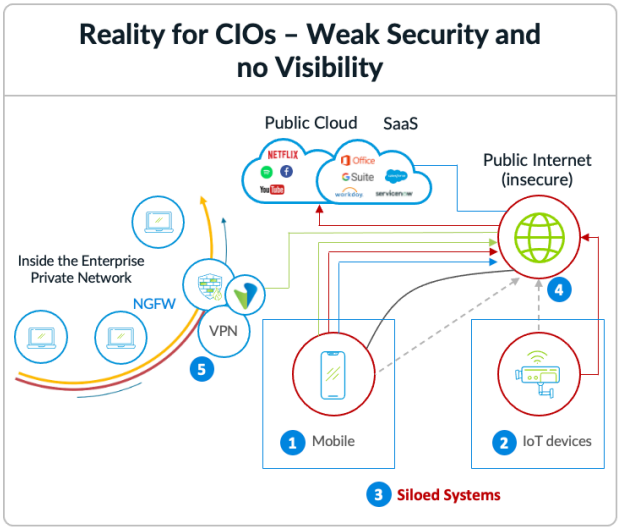
Table of Content

What is SASE-on-SIM and why is it important?

In today's rapidly evolving business landscape, enterprise mobility has become an indispensable tool for organizations to stay competitive and efficient. With the rise of private mobility, which refers to mobility solutions that are made available to the enterprises, organizations are finding new ways to enhance their operations and achieve better outcomes. This white paper explains how Versa SASE with various technologies provides such a foundation for Private mobility use case scenarios.

However, Service Providers have faced several challenges to deliver private mobility with optimal user experience and data privacy to enterprises, when using traditional solutions for IoT and Mobility projects.

1. Mobile with VPN Clients: A hassle for the IT team to manage another app.
2. VPN clients not compatible with all IoT devices
3. Access & protection for mobiles/IoT are siloed solutions (additional $$$)
4. Vulnerability gaps with devices on a network with no control and visibility
5. Additional expense of purchasing VPN concentrator and licenses



A few key challenges are the following:

- Dependency on software clients to effectively access internal applications when outside the enterprise premises. This leads to inconsistent application and security experience and added operational complexity for IT to manage the lifecycle of software clients
- Most IOT devices are closed box systems which do not allow the installation of additional software clients and agents. This leads to potential gaps in security landscape which could be exploited by threat actors.
- Legacy VPN concentrator technologies cannot provide effective segmentation and gives wholesale access to the entire network which increases overall risk to the organization.
- Enterprise IT teams do not have visibility of network activity when devices are outside enterprise network and are not connected to the VPN.
- Segregated security solution with perimeter-based security. People tend to compare the perimeter-based security with ZTNA. The latter has attracted a lot of the industrial interests as it was released, reason is simple and as its name indicated, Trust no one until policy permits.

Service Provider Use Case Scenarios

For Service Providers, Private mobility delivers low latency distributed security edges for retail use cases at a fraction of the cost. Some key use case scenarios where service providers can deliver contextual, risk based security with optimal user experience are:

Industry	Use Case Scenarios
Smart Cities, Government, Municipalities	Cameras, Sensors, Smart Billboards, Water meters, Gas Meters (Multi-tenancy, AI/ML Data Analytics, Traffic Steering)
Retail Industry	Scanners, IoT, Robots delivery (Obfuscation, Clientless SASE, Traffic Pattern Analysis)
Energy Sectors, Utilities	Autonomous Vehicles, Drones (Traffic Steering and Optimization)
Public Safety	Body Cams, Push-to-Talk (Real-Time Traffic Optimization, MOS-Based Traffic Steering)

For such Industry 4.0 use cases there is a need to introduce security at cloud scale, but at the same time ensure meeting aggressive SLA's through edge computing. For Service Providers it is imperative to make sure that that attack surface is protected, as proliferation of users and IoT devices are all an expanded attack surface.

Thus the entire SP mobility ecosystem needs to be secured with zero trust, where nothing is trusted by default. Versa SASE delivers the required mechanism for holistic Zero trust.

Versa SASE-on-SIM for Perimeter-less Private Mobile Network

Versa SASE allows organizations, especially for those who consume SASE-on-SIM (Private mobility) services to deploy SASE in the most flexible manner. Integration can be implemented

between light cloud to heavy cloud, to light branch, or to heavy branch deployment options, including in packet core networks.

The below diagram illustrates a classical use case where Versa SASE Gateway naturally fits into a packet core network performing network segmentation and traffic inspection.

When Versa SASE Gateways are introduced into the network, additional layers of intelligences along with benefits are made available to the enterprises, such as:

- SD-WAN Awareness - perfect for inter-branch communications.
- Built-in Security – Selectively enable NGFW, URL Filtering, UTM functions
- Traffic Steering – Break out traffic to Internet Locally, Remote Breakout at Hub/DC
- SaaS intelligence – SaaS Monitoring and Optimization

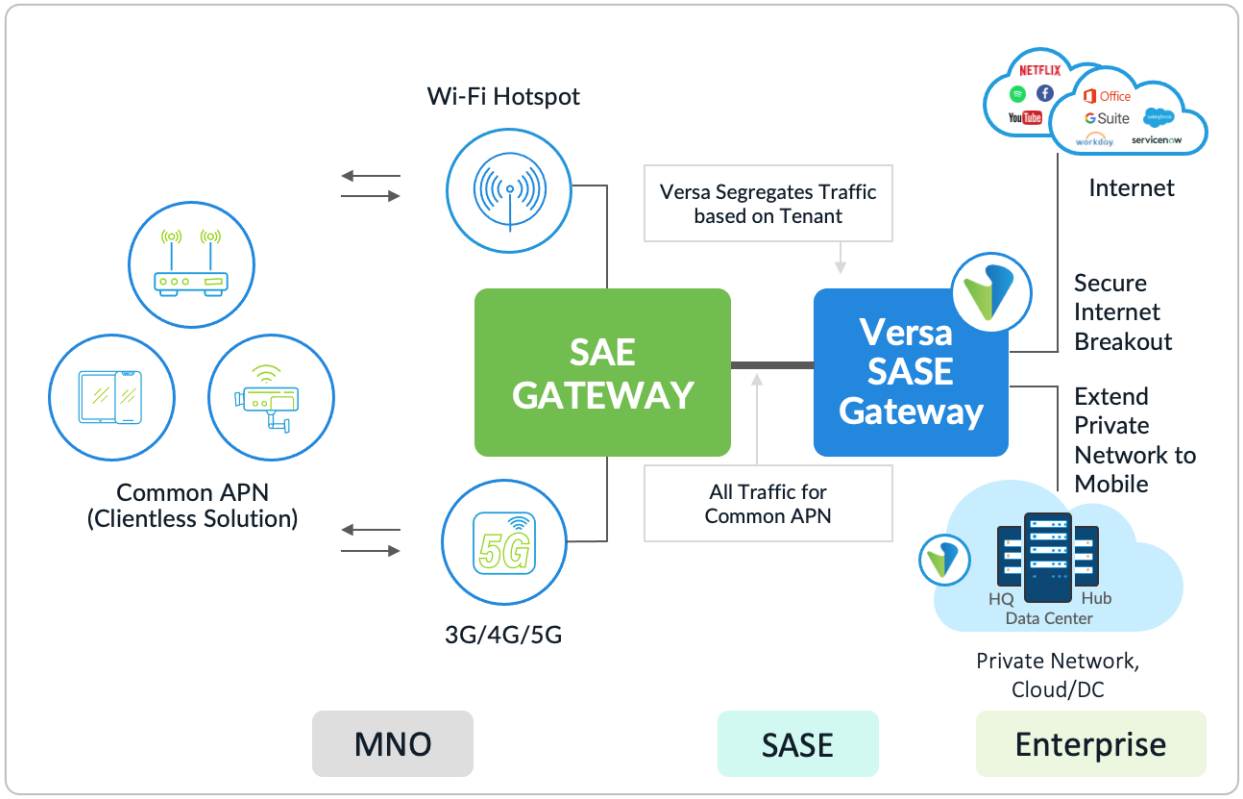


Figure – Modernized Packet Core Network with Versa SASE Gateway

Architecture and traffic flows

Requiring minimal to no infrastructure change, the Versa solution can seamlessly fit into Mobile Network Operator (MNO)'s existing networks by adding a "SASE" domain. From Control-plane perspective, MNO Operation team will benefit from Versa fully opened RESTful API to auto provision new endpoints via IMEI/IMSI, such information will be populated across Versa gateways in the SASE domain.

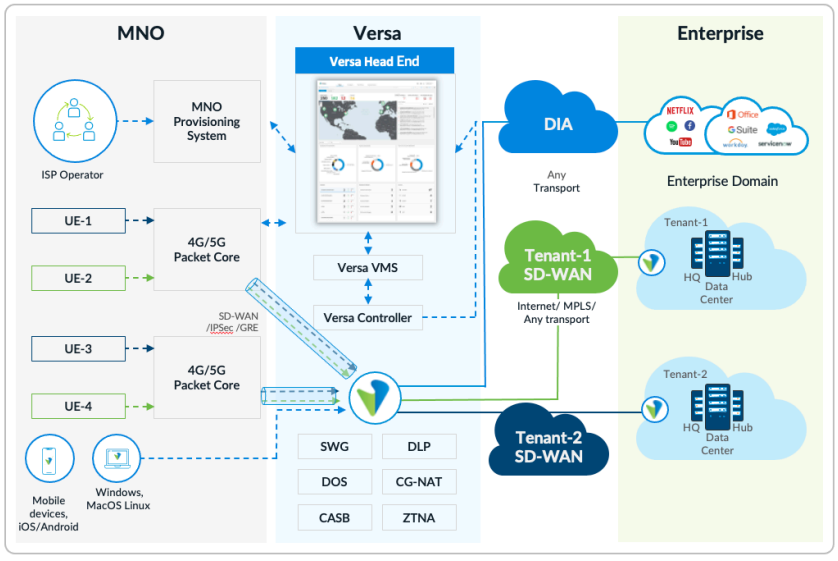
From data-plane perspective, Versa SASE Gateway segregates the traffic to specific tenant based on the IP address and device information (i.e., IMSI/IMEI). All traffic destined to enterprise network is sent to Enterprise private network over secure tunnel (SD-WAN or IPsec). Any traffic going to internet could be NAT'ed before sending packets to the Internet. All traffic can be securely inspected as per policy configuration.

Versa SASE Benefits

In general, Versa SASE enables organizations to securely connect Devices (IoT, UE's, Sensors, etc.) to branch offices, users, applications, and devices regardless of their location. SASE include many networking and network security services, and several capabilities found in SASE, such as SD-WAN and SWG, have been leveraged by organizations as industry best practices for several years. SASE transforms the traditional networking model of networking and security capabilities being service chained together. SASE enables organizations to adopt an architecture that connect, secure, and monitor applications and users where they exist.

Key Versa SASE services available via the cloud, on-premises, or as a blended combination of both include, but are not limited to:

Versa Services	
Software-Defined Wide Area Networking (SD-WAN)	A software-defined architecture for the Wide Area Network (WAN) increases network performance and agility.
Zero Trust Network Access (ZTNA)	Secure and private connectivity to corporate applications while implementing a least privileged model to access.
Secure Web Gateway (SWG)	Gateway protection against internet threats preventing unsecured traffic from compromising internal networks and users.
Cloud Access Security Broker (CASB)	Policy enforcement that secures data flowing between users and cloud applications to comply with corporate and regulatory requirements.
Firewall-as-a Service (FWaaS)	A cloud service that delivers firewall and other network security capabilities to inspect and control all network traffic
Remote Browser Isolation (RBI)	A risk mitigation solution that moves the execution of users' browsing activity to a remote server hosted in the cloud or on-premises



- Requires *No* to *Minimal* changes to existing MNO Infrastructure
- Tenant identification data configured by MNO's provisioning system.
- Versa SASE gateways maps the user's traffic on to the right SD-WAN overlay or break it out locally after applying security policies.
- Device and user information is obfuscated before sending to cloud.
- Multi-tenancy across entire communication(Control, Data, Management and Analytics Planes)
- No VPN Client, and support mobility from 4G/5G to Wi-Fi

Minimal to No Infrastructure change

Versa Solution can be easily deployed with minimal and even no change to be made within MNO's existing mission critical infrastructure, the new "SASE domain" is only added as an extension to the existing MNO network. This greatly increases "time-to-market" efficiency, and harmless to network uptime commitment.

Securely bridging "Shared" and "Private" infrastructure

Versa Solution acts as the "glue" between the "shared" endpoint infrastructure on the left and "private" enterprise infrastructure on the right. The unified SASE infrastructure with genuine multi-tenancy minimizes the need of repetitive deployment for each new customer, while many value-added services mentioned previously (SD-WAN Aware, Built-in Security, etc.) are being offered.

Clientless SASE

Many types of clients in SASE-on-SIM deployment are unintelligent, such as cameras, sensors, thin clients. As these endpoints attach to field radio network, Versa SASE Gateways utilize the IMSI/IMEI along with IP address information shared by mobile operators for tenant's traffic identification, endpoints are now mapped to the correct network segment, and ready for further processing.

SD-WAN Awareness

Versa SASE Gateways are part of Versa ecosystem, and therefore natively SD-WAN-aware. As soon as field endpoints are mapped to the correct tenants and network segment, they can be managed by remote network operators who belong to the same tenant(enterprise). Additional Versa SD-WAN intelligence such as protected local breakout (DIA), and SaaS optimizations can also be enabled.

Network Obfuscation

All Versa SASE Gateway comes with **Network Obfuscation feature**, which perfectly prevent lateral movement of network attack if any of the endpoint is compromised. This enforces devices and user information are always isolated and protected.

Security and Policy Enforcement

Versa SASE Gateway comes with built-in security that supports modern security protocols like CASB, NGFW, UTM, URL Filtering etc. As endpoint traffic going through the Versa SASE Gateways, policy can be enforced based on many factors:

- Source/Destination Address
- Source/Destination Protocol and ports
- Time of the day
- Geo-location
- User/Group

Importantly, policies are on per-tenant basis, each tenant in the deployment receives different sets of policies based on requirement.

Why Versa Networks?

Versa SASE provides an excellent choice for enterprises, mobile network operators, and partners to build their own private SASE service on their own premises or in their own private cloud. This flexibility creates tremendous opportunities to gain full control over the services, yet take advantage of performance and capabilities of the market leading Versa SASE solution.

End-to-End Visibility and Control

Through a single-pane-of-glass interface, SASE offers complete visibility into users, devices, and applications across the entire network- whether on-premises or in the cloud.

Consistent Security Enforcement

SASE enables security teams to bring cloud platforms, data centers, branch offices, remote and mobile users under one umbrella and protect them with one unified security policy pushed to every user on any device, anywhere.

Optimized Application Performance

Versa SASE has application awareness and dynamic traffic steering capabilities that monitor traffic patterns in real-time to analyze performance parameters such as latency, jitter, and packet loss. Based on these parameters, Versa SASE automatically routes traffic over the ideal transport route. In doing so, it ensures all applications, especially voice and video, run seamlessly and reliably for an uninterrupted user experience.

Lower Capital and Operational Expenses

Installing commodity point products in branch locations is costly. Enabling Versa on OEM Hardware, Whitebox, Cloud or VM can dramatically bring down the total cost of ownership, and increase flexibilities for enterprises.