Versa SASE Fabric

Contents

Overview 2
SASE evolution 2
SASE Architectures. 3
Versa SASE Fabric. 4
The Orchestration Plane 4
The Operations Plane. 4
The Data Plane 5
The Control Plane 5
The Overlays 8
Summary 8

Overview

The Versa SASE Fabric, a part of the Versa Secure Access Fabric, is an interconnected, policy-aware, distributed system where networking, security, identity, analytics, and orchestration operate as a single unified platform. It is a globally distributed SASE architecture that interconnects Versa SASE Gateways, at 100+ global PoPs, through an encrypted software-defined fabric to deliver unified networking and security services including SD-WAN, ZTNA, SWG, CASB, and FwaaS.

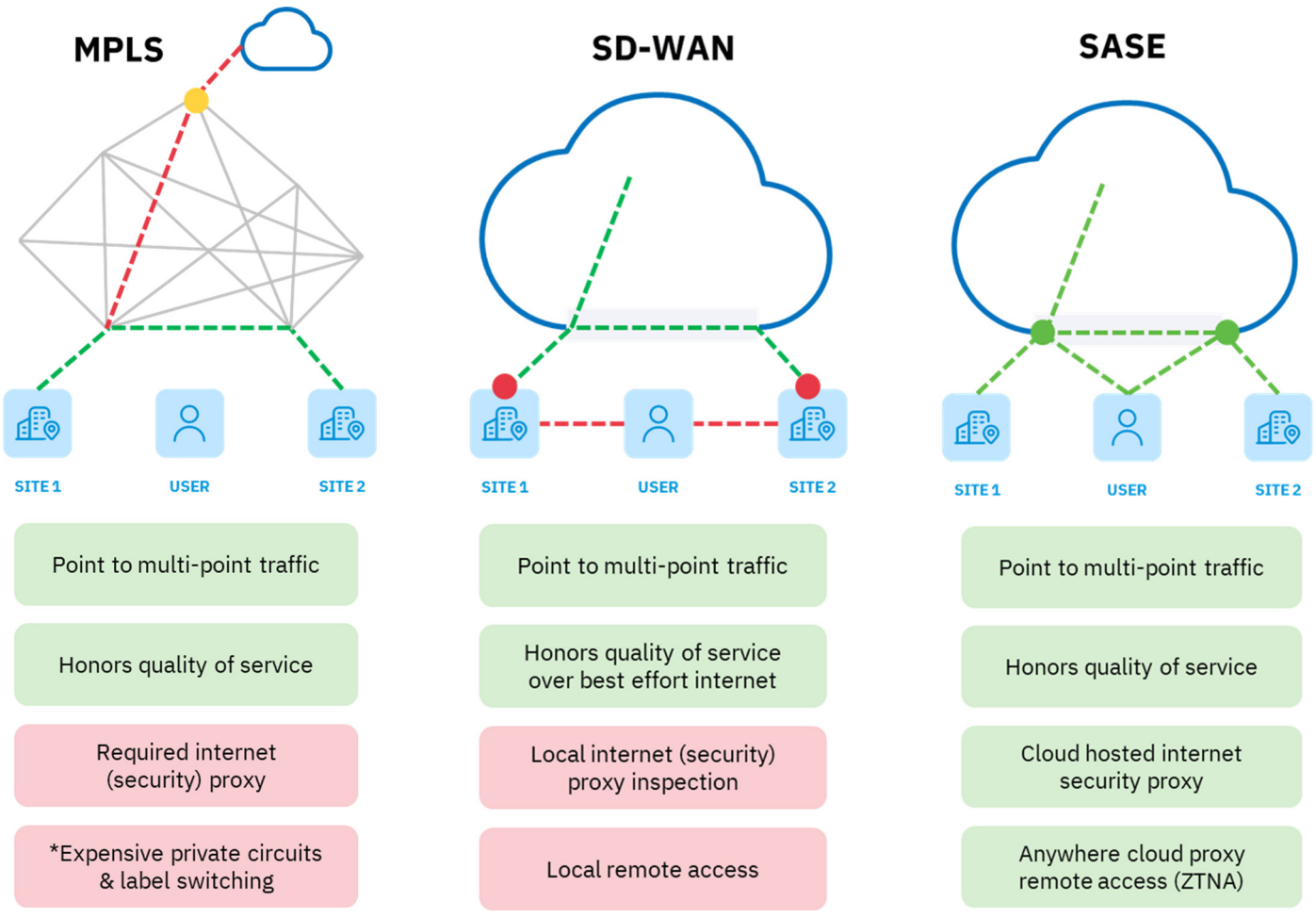
SASE evolution

MPLS was the point-to-multipoint network approach for many companies before SASE. It could glue access between global sites while providing guaranteed quality of service for mission critical application flows. At same time MPLS services were expensive as providers operated complex label switching networks.

As companies moved workloads to the cloud and consumed more SaaS/PaaS/IaaS a flaw was revealed in Enterprise network architectures in that internet security for sites required inspection via central internet proxies.

SD-WAN introduces a means of providing quality point to multi-point connectivity over best effort internet with security inspection at the site level. It significantly improved networking and security, but it did not solve giving remote users secure ubiquitous access.

SASE combines both technologies, moving security inspection to the cloud edge while giving remote users secure anywhere access. Yet once traffic reaches the cloud edge, SASE implementations diverge.



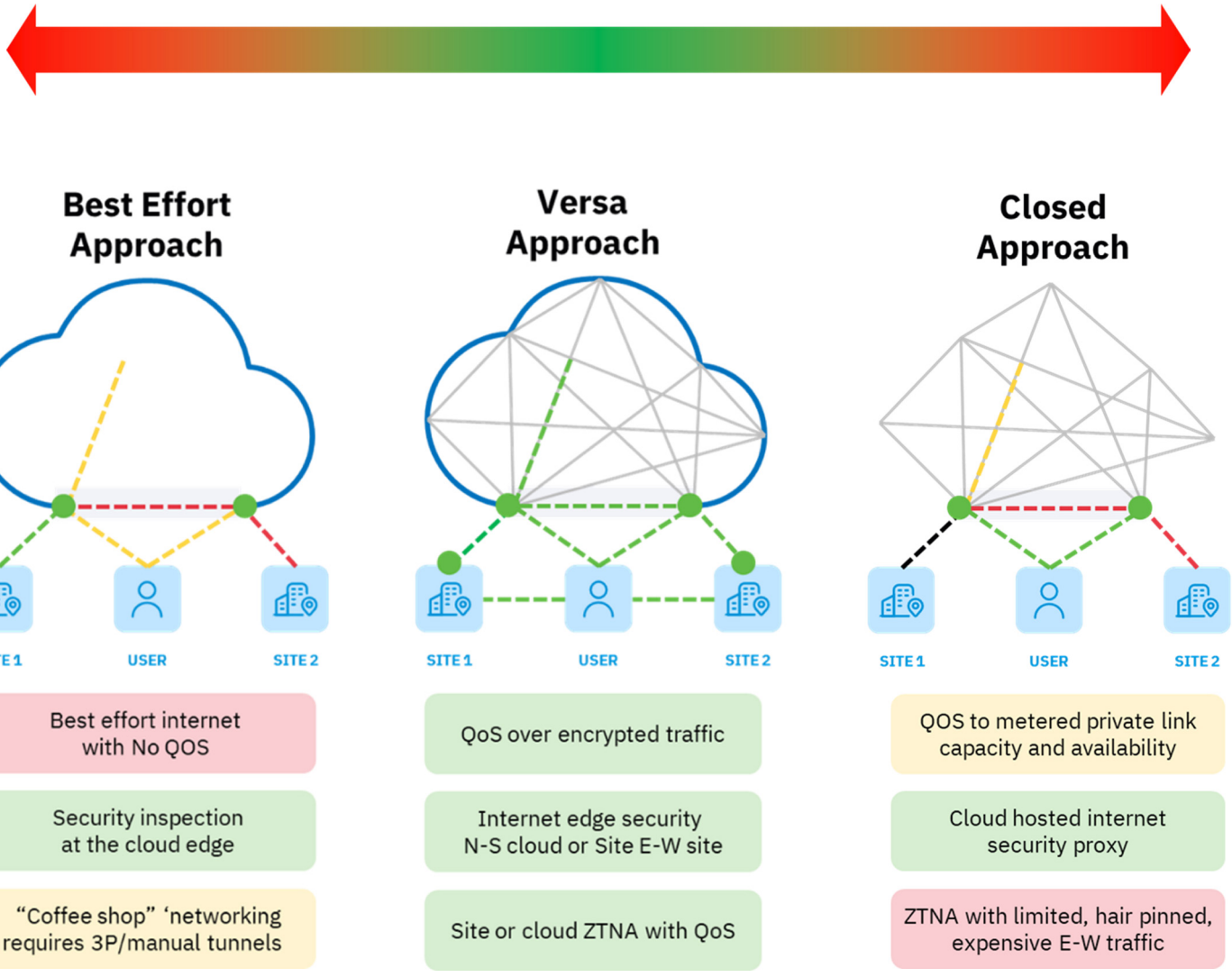
SASE Architectures

On one end of the spectrum cloud-focused vendors took the approach of, post security inspection, “dumping” traffic off for the best effort internet to find the “best available” path based on BGP preferences for the most part like shortest AS path.

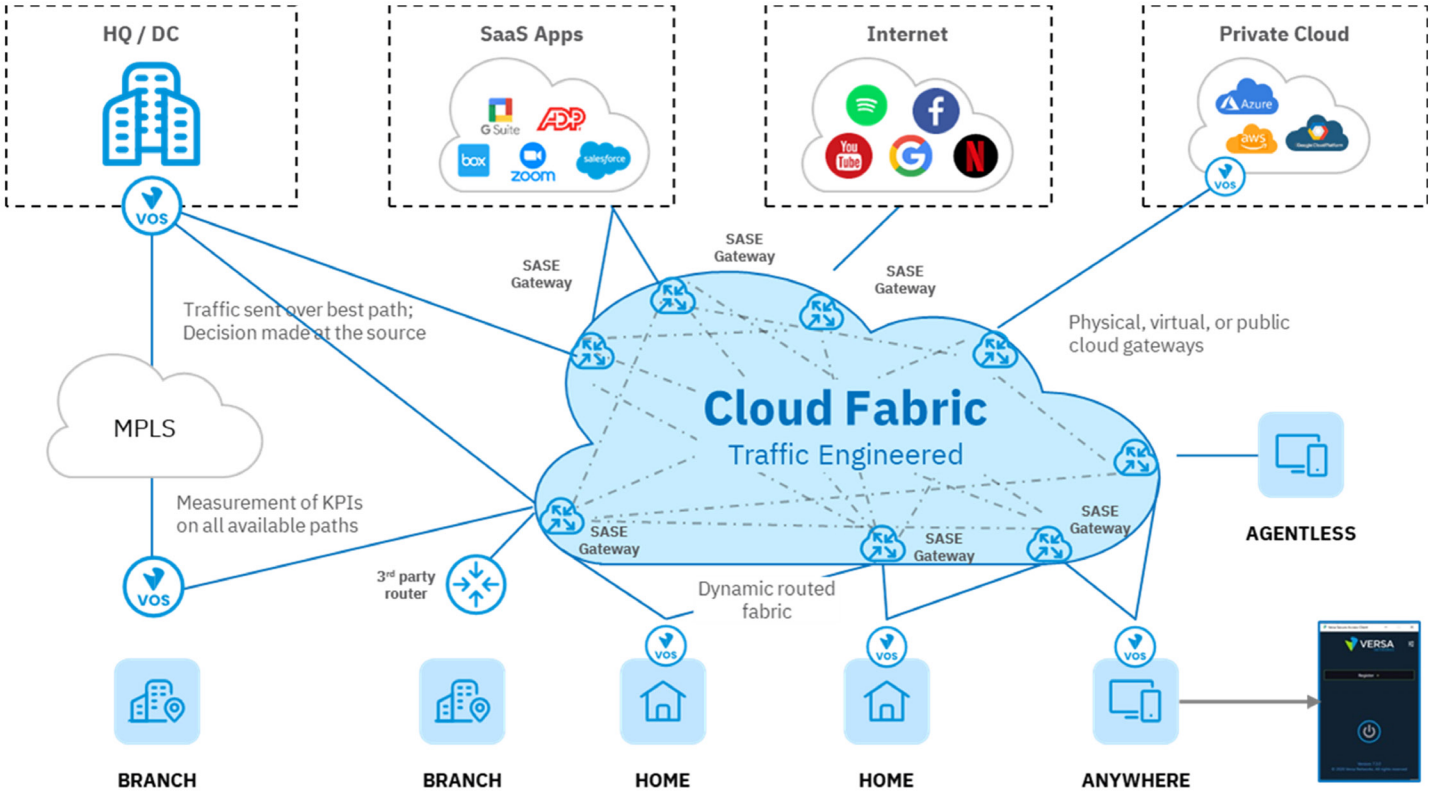
On the other end vendors built their own proprietary private (MPLS-like) backbone. Yet traffic is at the mercy of their private network routes. Also, east-west traffic that might take a shorter path between sites must hairpin through their cloud adding latency and cost for service contracts which are all metered according to bandwidth consumption.

Versa SASE Fabric combines the best of both approaches with a dynamic secure platform.

SASE vendors chose different approaches architecturally



Versa SASE Fabric



To better understand the Versa SASE Fabric, we can consider its functional “planes”:

- Multi-tenant **Orchestration Plane** for configuration and management
- Granular **Operations Plane** for 360-degree monitoring, telemetry, and reporting
- Distributed scalable **Data Plane** for traffic forwarding + security inspection
- Intelligent **Control Plane** for routing decisions and path selection

The Orchestration Plane

This plane allows teams to define access intent, application policy, risk tolerance, traffic steering rules, Inspection depth, and segmentation strategy.

Then push it across the entire fabric. With NO duplicated firewall rules, NO mismatched branch configs, and NO remote-user exceptions. It’s unified policy model enforced everywhere.

The Operations Plane

The Operations Plane handles user behavior visibility, application performance metrics, risk scoring, traffic pattern learning, and policy effectiveness feedback.

Because all nodes share a common architecture, analytics aren’t stitched together logs from unrelated systems. They’re native signals from the same distributed runtime. That allows closed-loop optimization. That feedback loop is what makes a fabric adaptive.

- **Capacity** – Versa provides bandwidth based on customer needs with a EULA that includes “Versa Secure Access Fabric (VSAF) subscription usage guidelines - Versa EULA
- **SLAs** – Versa provides service level agreements for fabric connectivity - Versa SLAs

The Data Plane

Every node in the Versa Fabric, whether a branch appliance or cloud gateway, runs the Versa Operating System (VOS). It includes broad capabilities from forwarding and application steering to security inspection of data flows including Next-generation firewall, DLP, CASB, IPS, URL filtering, SWG, or ZTNA.

This means enforcement is not centralized in a single cloud choke point, rather local when needed or cloud-delivered when optimal. Security follows the session by nature in the Versa fabric.

The Control Plane

The control plane, based on Versa SD-WAN, is hosted on instances of VOS uses MP-BGP to advertise site and route information to branch devices so they can automatically discover each other and build overlay tunnels, without sitting in the data path.

It operates on two distinct network layers:

Underlay - the native routes available via an IGP or EGP.

Interface	Role
vni-0/x.y	Physical WAN interface
tvi-0/x.y	Logical SD-WAN transport interface
VRF	Tenant routing domain

```
admin@Branch3-cli> show route routing-instance INET1-Transport-VR

Routes for Routing instance : INET1-Transport-VR  AFI: ipv4  SAFI: unicast

Codes: E1 - OSPF external type 1, E2 - OSPF external type 2
IA - inter area, iA - intra area,
L1 - IS-IS level-1, L2 - IS-IS level-2
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
RTI - Learnt from another routing-instance
SUMM - SUMMARY/AGGREGATE route
+ - Active Route

Prot   Type  Dest Address/Mask   Next-hop        Age      Interface name     Nexthop name
----   ----  -----------------   --------        ---      --------------     ---------------
DHCP   N/A  +0.0.0.0/0           10.70.0.1       01:52:31 vni-0/0.0

conn   N/A  +10.70.0.0/16        0.0.0.0         01:52:31 vni-0/0.0

local  N/A  +10.70.198.123/32    0.0.0.0         01:52:31 directly connected

conn   N/A  +169.254.0.2/31      0.0.0.0         01:52:54 tvi-0/602.0

local  N/A  +169.254.0.2/32      0.0.0.0         01:52:54 directly connected

BGP    N/A  +172.16.3.0/24       169.254.0.3     01:52:35 tvi-0/602.0



Routes for Routing instance : INET1-Transport-VR  AFI: ipv6  SAFI: unicast
```

Overlay - the routes centrally managed by SD-WAN

Routes are dynamic and paths are driven based on performance metrics like loss, latency, or jitter not static metrics

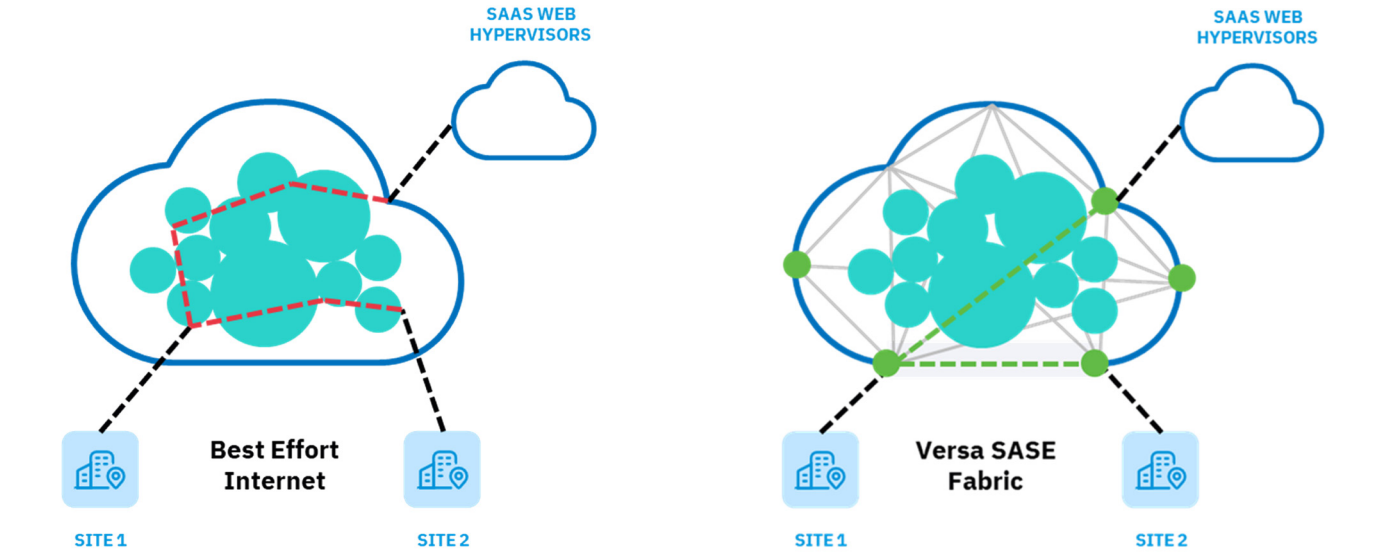
```
Routes for Routing instance : AcmeMarketing-Control-VR  AFI: ipv4  SAFI: unicast

Routing entry for 172.16.3.0/24
   Peer Address       : 100.64.0.2
   Route Distinguisher: 168L:232
   Next-hop           : 100.64.3.215
   VPN Label          : 24704
   Local Preference   : 110
   AS Path            : N/A
   AS Path(. notation): N/A
   Origin             : Igp
   MED                : 0
   Community          : N/A
   Extended community : target:168L:168
```

Versa SD-WAN provides a broad feature set to optimize flow transport:

- **Secure, dynamic, encrypted VPN overlays** — Versa builds encrypted SD-WAN overlay tunnels across multiple access links so branches and hubs can connect securely and adaptively over different transports.
- **Application detection and visibility** — Versa identifies applications and provides visibility into them so traffic can be monitored, classified, and controlled by policy.
- **Application traffic control, traffic engineering, and application QoS** — Versa applies policy-based steering and application-aware QoS so traffic is prioritized, queued, scheduled, and routed according to app requirements and link conditions.
- **SLA-based path measurement** — Versa continuously measures SLA metrics such as jitter, latency, packet loss, MOS, and link utilization and can shift traffic when a path violates policy thresholds.
- **Cloud and direct internet access (DIA)-destined traffic optimizations** — Versa optimizes traffic headed directly to the internet or cloud destinations so branches can use better-performing exits rather than forcing everything through a central site.
- **Optimized voice service using MOS scores** — Versa measures voice and collaboration quality with MOS and can automatically steer traffic to improve call quality.
- **Accelerated applications using FEC or packet cloning** — Versa uses FEC and packet cloning to reduce retransmissions and improve performance and resiliency on lossy or congested links.
- **Optimized access to SaaS cloud** — Versa measures SaaS path performance, distributes that intelligence with TELS, and dynamically selects the best next hop or gateway to improve SaaS experience.
- **Distributed traffic engineering with TELS** — Versa's Traffic Engineered Link State protocol distributes network and SaaS performance information to edge nodes so they can calculate end-to-end path quality and choose the best policy-compliant path.
- **Packet striping** — Versa can stripe traffic across multiple links so several underlays behave more like one larger logical pipe for better throughput.
- **Zero-touch provisioning (ZTP)** — Versa can automatically provision and configure new branch devices, reducing manual deployment work.
- **Active/active transport and load balancing** — Versa supports active/active transport usage and load balancing so multiple WAN links can be used simultaneously instead of sitting idle as backup only.
- **Flexible topology support** — Versa supports full-mesh, partial-mesh, hub-and-spoke, controller-behind-branch, branch-behind-branch, and custom topologies for different enterprise and service-provider designs.
- **Multitenancy with RBAC** — Versa supports multitenant isolation with separate routing instances, overlays, policies, and role-based access control, which is especially important for managed service providers.
- **Fabric flow control and adaptive shaping** — Versa can detect sustained congestion across SD-WAN sites and use the control plane to throttle sources and enforce traffic policies more consistently across the fabric.
- **Service chaining and third-party integration** — Versa can chain native and third-party network functions so application traffic can be sent through the right sequence of services as needed.
- **Tunnel-less SD-WAN for satellite-type environments** — Versa documents tunnel-less SD-WAN deployments for satellite-based WAN links and similar use cases where traditional tunneling may be less desirable.
- **Integrated routing and broad WAN-edge functionality** — Versa combines SD-WAN with carrier-class routing, Layer 2/Layer 3 features, and integrated security on the same VOS platform.
- **Application-specific optimizations** — Versa supports per-application optimization behavior, including TCP optimization profiles that mitigate latency and packet loss for TCP-based applications.

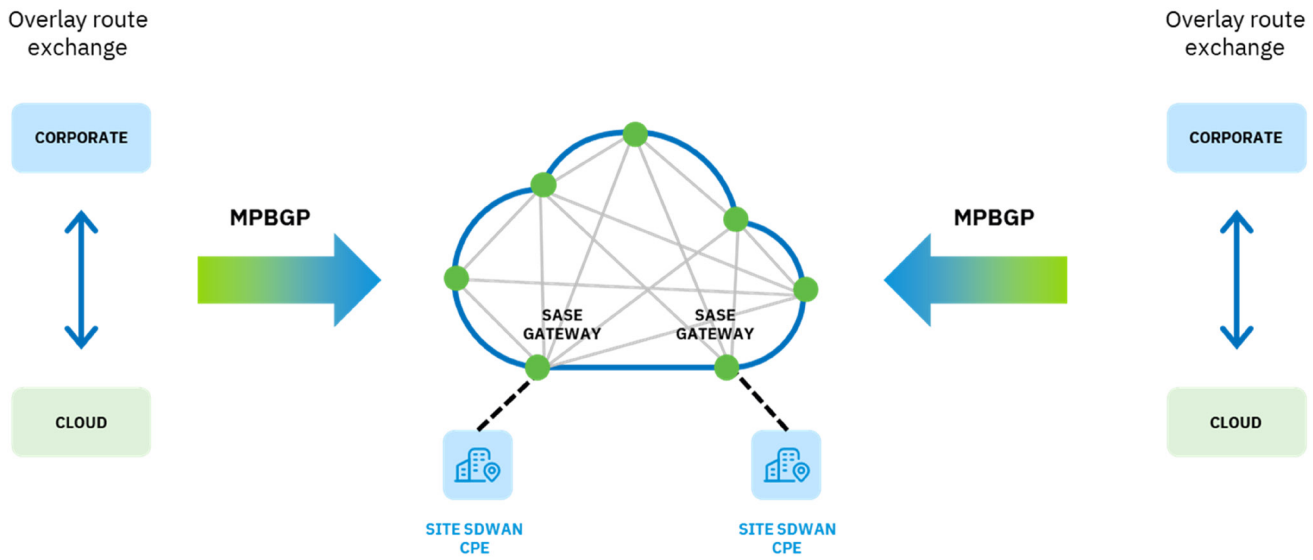
- **Application acceleration** - improves connection across Versa Cloud Gateways with TCP, Forward Error Correction, and caching to sites like:
  - ✓ SaaS (Office365, Google Suite, Salesforce, Workday, ServiceNow, etc.)
  - ✓ Web (Facebook, CNN etc.)
  - ✓ Hypervisors (AWS, GCP, Azure)

Peering - The internet consists of peering arrangements between different service providers. Through diverse transit and peering agreements Versa's own private SD-WAN driven backbone can create optimal paths for Versa customer's to consume https://bgp.tools/as/400318#asinfo



Customer traffic over best effort internet may take sub-optimal paths

Through peering and transit agreements Versa SASE Fabric provides optimized paths, over a dynamic encrypted backbone, after security inspection at the edge



The Overlays

Customer tenants enjoy the same Versa SD-WAN technology to optimize their network and their overlay becomes an extension of the Versa SASE Fabric

Versa customer tenant SD-WAN site CPEs and the Versa SASE Fabric exchange **overlay routes** using MP-BGP across the SD-WAN tunnel interfaces, allowing enterprise site prefixes and SASE service prefixes to be dynamically distributed across the fabric.

Site CPEs advertise their enterprise networks and these become reachable from SASE gateway nodes. In turn once they learn routes from SASE fabric the tenants data plane is extended to it and traffic can be forwarded over overlay tunnel interfaces.

Summary

Versa SASE Fabric provides a unified, globally distributed architecture that seamlessly integrates security services into a single routing fabric, enabling consistent security policy, optimal traffic steering, and simplified operations across users, branches, and applications.

Visit the Versa Secure Access Fabric datasheet to learn more or see it for yourself with a demonstration from a Versa SASE Fabric expert.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

©2026 Versa Networks, Inc. All rights reserved. Portions of Versa products are protected under Versa patents, as well as patents pending. Versa Networks and FlexVNF are trademarks or registered trademarks of Versa Networks, Inc. All other trademarks used or mentioned herein belong to their respective owners.

Part# WP_SASEFAB-01.0